(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2001265771 A**

(43) Date of publication of application: **28.09.01**

(51) Int. Cl **G06F 17/30**
G06F 12/14
G06F 17/60

(21) Application number: **2000079411**

(22) Date of filing: **22.03.00**

(71) Applicant: **NIPPON TELEGR & TELEPH CORP <NTT>**

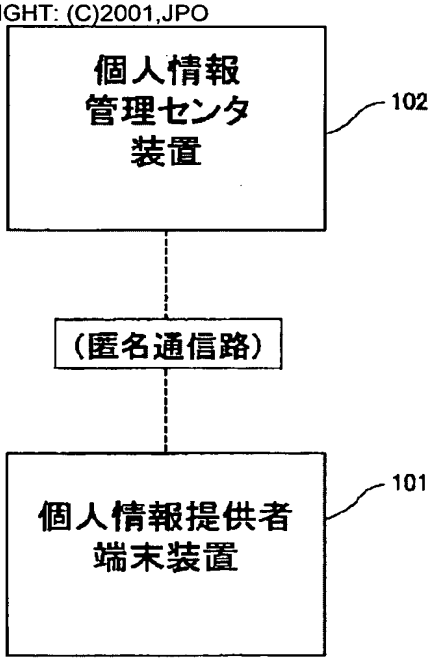
(72) Inventor: **YAMAMOTO KANA**
HORIOKA TSUTOMU
TAKASHIMA YOICHI

(54) **DEVICE AND METHOD FOR MANAGING PERSONAL INFORMATION AND RECORDING MEDIUM RECORDING PROGRAM FOR EXECUTING THE DEVICE OR METHOD**

(57) Abstract:

PROBLEM TO BE SOLVED: To solve the problem that is a hand to protect privacy and there is the danger of leak to a third person in personal information provision on a network through a managing center.

SOLUTION: Personal information on personal information provider terminal equipment 101 to provide personal information to the other person is registered in a personal information managing center device 102 after being divided into partial personal information, which can not be related with a specified individual respectively singly and is meaningless, and by holding the relation of such information only on the terminal of a personal information provider, the privacy of the personal information provider can not be grasped in the personal information managing center. Besides, the set of the identifier of the partial personal information registered in the personal information managing center and personal information acquisition agreement conditions is provided to a personal information user and only in the case of matching to the acquisition agreement conditions, personal information is provided.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－265771
（P2001－265771A）
(43)公開日　平成13年９月28日(2001.9.28)

(51)Int.Cl.⁷	識別記号	FI		テーマコード（参考）
G06F 17/30	120	G06F 17/30	120A	5B017
	170		170Z	5B049
	340		340A	5B075
12/14	320	12/14	320B	
17/60	172	17/60	172	

審査請求　未請求　請求項の数22　ＯＬ　（全 24 頁）　最終頁に続く

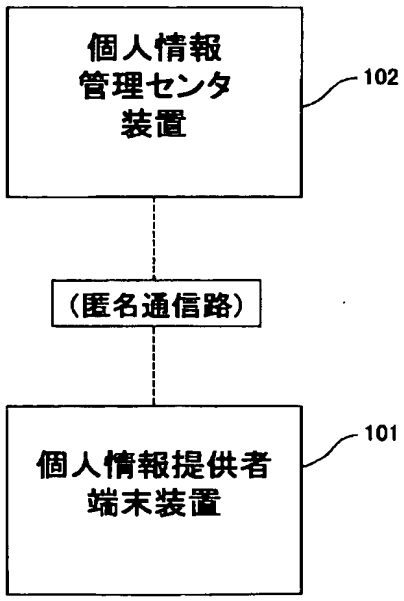
(21)出願番号　特願2000－79411(P2000－79411)
(22)出願日　平成12年３月22日(2000.3.22)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　山本　泰
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　堀岡　力
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(74)代理人　100062199
弁理士　志賀　富士弥　（外１名）

最終頁に続く

(54)【発明の名称】　個人情報管理装置、個人情報管理方法、及び個人情報管理装置または方法を実行するプログラムを記録した記録媒体

(57)【要約】
【課題】　管理センタを介してネットワークによる個人情報提供では、プライバシを守るのが難しいし、第三者に漏れる恐れがある。
【解決手段】　個人情報を他者に提供しようとする個人情報提供者端末装置１０１に関する個人情報を、それぞれ単独では特定の個人との関連づけができずに意味をなさない部分個人情報に分割した上で個人情報管理センタ装置１０２に登録し、それらの間の関連は個人情報提供者の持つ端末でのみ保持することで、個人情報管理センタでは個人情報提供者のプライバシを把握できなくする。また、個人情報利用者に対しては、個人情報管理センタに登録された部分個人情報の識別子と、個人情報取得許諾条件をセットにして提供し、取得許諾条件に合う場合にのみ個人情報を提供する。



1

【特許請求の範囲】

【請求項１】　個人情報提供者端末装置で提供する個人情報を通信手段を介して個人情報管理センタ装置に登録し、個人情報利用者端末装置が前記個人情報を通信手段を介して取得して利用する個人情報管理装置であって、前記個人情報提供者端末装置は、入力された個人情報を単独では特定の個人との関連づけができずに意味をなさない部分個人情報に分割するための個人情報分割手段と、この部分個人情報を前記個人情報管理センタ装置に送信する手段と、前記個人情報管理センタ装置で部分個人情報に対して生成した部分個人情報識別子を受信する手段と、前記受信した部分個人情報識別子によって表される部分個人情報の内容と対応づけて保存する部分個人情報関連記憶手段と、提供しようとする部分個人情報に対応した部分個人情報識別子を前記部分個人情報関連記憶手段から取得して前記個人情報利用者端末装置に送信する手段とを備えたことを特徴とする個人情報管理装置。

【請求項２】　請求項１の個人情報管理装置において、前記個人情報提供者端末装置は、前記部分個人情報識別子を部分個人情報関連記憶手段から取り出して前記個人情報管理センタ装置に送信する手段と、前記個人情報管理センタ装置から部分個人情報識別子に対応する部分個人情報を受信する手段と、前記受信した前記部分個人情報を出力する手段を備えたことを特徴とする個人情報管理装置。

【請求項３】　請求項１の個人情報管理装置において、前記個人情報提供者端末装置は、変更しようとする個人情報を入力する手段と、前記個人情報分割手段によって分割された部分個人情報の内容に応じた部分個人情報識別子を前記部分個人情報関連記憶手段から検索する手段と、前記部分個人情報とその識別子を対にして前記個人情報管理センタ装置に送信する手段とを備えたことを特徴とする個人情報管理装置。

【請求項４】　請求項１の個人情報管理装置において、前記個人情報提供者端末装置は、前記部分個人情報関連記憶手段から提供したい部分個人情報に対応した部分個人情報識別子を取り出す手段と、前記個人情報利用者端末装置にどのような部分個人情報をどのような条件で提供するのかを表す部分個人情報利用許諾情報を生成する手段と、前記個人情報利用者端末装置に対して前記部分個人情報利用許諾情報を送信する手段とを備えたことを特徴とする個人情報管理装置。

【請求項５】　請求項３の個人情報管理装置において、前記個人情報提供者端末装置は、提供する個人情報を前記個人情報分割手段で分割した部分個人情報を暗号化するための暗号鍵を生成する手段と、各部分個人情報を前記暗号鍵を用いて暗号化する手段と、前記暗号化部分個人情報をそれぞれ別個に前記個人情報管理センタ装置に送信する手段と、前記個人情報管理センタ装置で生成し

2

受信した部分個人情報識別子を、それによって表される部分個人情報の内容および、暗号化に用いた前記暗号化鍵と対応づけて前記部分個人情報関連記憶手段に保存する手段とを備えことを特徴とする個人情報管理装置。

【請求項６】　個人情報提供者端末装置で提供する個人情報を通信手段を介して個人情報管理センタ装置に登録し、個人情報利用者端末装置が前記個人情報を通信手段を介して取得して利用する個人情報管理装置であって、前記個人情報管理センタ装置は、個人情報をを単独では特定の個人との関連づけができずに意味をなさない部分個人情報に分割した部分個人情報を前記個人情報提供者端末装置から受信する手段と、前記受信した部分個人情報に識別子を生成する識別子生成手段と、該生成した部分個人情報識別子と前記部分個人情報とを対応させて保存する部分個人情報記憶手段と、前記部分個人情報識別子を個人情報提供者端末装置に送信する手段と、前記個人情報利用者端末装置から受信した部分個人情報識別子に対応する部分個人情報を前記部分個人情報記憶手段から検索する手段と、前記検索された部分個人情報を前記個人情報提供者端末装置に送信する手段とを備えたことを特徴とする個人情報管理装置。

【請求項７】　請求項６の個人情報管理装置において、前記個人情報管理センタ装置は、前記個人情報提供者端末装置が変更しようとする前記部分個人情報と該部分個人情報の内容に応じた部分個人情報識別子を受信する手段と、前記受信した部分個人情報識別子を用いて前記部分個人情報を検索してその値を受信した部分個人情報の値に変更する手段とを備えたことを特徴とする個人情報管理装置。

【請求項８】　請求項６の個人情報管理装置において、前記個人情報管理センタ装置は、個人情報利用者端末装置が利用しようとする部分個人情報に対応した部分個人情報利用許諾情報を受信する手段と、前記受信した部分個人情報利用許諾情報が、当該個人情報利用者端末装置に対して、指定された部分個人情報の利用を許諾したものかどうかを検証する利用条件判断手段と、前記検証が成功した場合に前記部分個人情報利用許諾情報に指定された部分個人情報識別子に対応する部分個人情報を前記部分個人情報記憶手段から検索する手段と、前記検索した部分個人情報を前記個人情報利用者端末装置に送信する手段とを備えたことを特徴とする個人情報管理装置。

【請求項９】　請求項８の個人情報管理装置において、前記個人情報管理センタ装置は、前記受信した部分個人情報利用許諾情報が条件を満たしていることを確認したときに該部分個人情報利用許諾情報に指定された部分個人情報識別子に対応する部分個人情報を前記部分個人情報記憶装置から検索する手段と、前記検索した部分個人情報の列の順序をランダムに入れ換える部分個人情報順序入換手段と、前記順序の入れ換えられた部分個人情報の列を前記個人情報利用者端末装置に送信する手段とを

備えたことを特徴とする個人情報管理装置。

【請求項１０】　請求項７の個人情報管理装置において、

前記個人情報管理センタ装置は、前記個人情報提供者端末装置が部分個人情報を暗号鍵を用いて暗号化した部分個人情報を受信する手段と、前記受信した暗号化部分個人情報に対応した部分個人情報識別子を生成する部分個人情報識別子生成手段と、前記生成した部分個人情報識別子と前記提供者暗号化部分個人情報とを対応させて前記部分個人情報記憶手段に保存する手段と、前記部分個人情報識別子を前記個人情報提供者端末装置に送信する手段とを備えたことを特徴とする個人情報管理装置。

【請求項１１】　請求項９の個人情報管理装置において、

前記個人情報管理センタ装置は、前記個人情報利用者端末装置が利用しようとする部分個人情報に対応した部分個人情報利用許諾情報を受信する手段と、前記受信した部分個人情報利用許諾情報が、当該個人情報利用者端末装置に対して、指定された部分個人情報の利用を許諾したものかどうかを検証する利用条件判断手段と、前記検証が成功した場合に前記部分個人情報利用許諾情報に指定された部分個人情報識別子に対応する部分個人情報を前記部分個人情報記憶手段から検索する手段と、前記検索した部分個人情報を前記個人情報利用者端末装置に送信する手段とを備えたことを特徴とする個人情報管理装置。

【請求項１２】　請求項１１の個人情報管理装置において、

前記個人情報管理センタ装置は、前記部分個人情報利用許諾情報に指定された部分個人情報識別子に対応する部分個人情報を前記部分個人情報記憶装置から検索する手段と、各提供者暗号化部分個人情報を個人情報管理センタ装置のみが知る鍵を用いて暗号化してセンタ暗号化提供者暗号化部分個人情報の列を得て前記個人情報利用者端末装置に送信する手段と、前記個人情報利用者端末装置から受信した前記利用者暗号化センタ暗号化部分個人情報の列に含まれる利用者暗号化センタ暗号化部分個人情報をそれぞれ鍵を用いて復号する手段と、前記復号した利用者暗号化部分個人情報の列の順序をランダムに入れ換える部分個人情報順序入換手段と、前記入れ換えた利用者暗号化部分個人情報の列を前記個人情報利用者端末装置に送信する手段とを備えたことを特徴とする個人情報管理装置。

【請求項１３】　個人情報提供者端末装置で提供する個人情報を通信手段を介して個人情報管理センタ装置に登録し、個人情報利用者端末装置が前記個人情報を通信手段を介して取得して利用する個人情報管理装置であって、

前記個人情報利用者端末装置は、前記個人情報提供者端末装置から提供したい部分個人情報に対応した部分個人情報識別子を受信する手段と、前記受信した個人情報識別子を部分個人情報識別子記憶装置に保存する手段と、前記保存した部分個人情報識別子を前記個人情報管理センタ装置に送信する手段と、前記送信に対して前記個人情報管理センタ装置から部分個人情報識別子に対応する部分個人情報を受信する手段と、該受信した部分個人情報を出力する手段とを備えたことを特徴とする個人情報管理装置。

【請求項１４】　請求項１３の個人情報管理装置において、

前記個人情報利用者端末装置は、前記個人情報提供者端末装置から提供したい部分個人情報についてどのような部分個人情報をどのような条件で提供するのかを表す部分個人情報利用許諾情報を受信する手段と、前記受信した部分個人情報利用許諾情報を部分個人情報利用許諾情報記憶手段に保存することを特徴とする個人情報管理装置。

【請求項１５】　請求項１３の個人情報管理装置において、

前記個人情報利用者端末装置は、利用したい部分個人情報に対応した部分個人情報利用許諾情報を前記部分個人情報利用許諾情報記憶手段から取り出す手段と、該取り出した前記部分個人情報利用許諾情報を前記個人情報管理センタ装置に送信する手段と、前記部分個人情報利用許諾情報に対して個人情報管理センタ装置報により指定された部分個人情報の利用を許諾したことを検証し、該部分個人情報利用許諾情報に指定された部分個人情報識別子に対応する部分個人情報を受信する手段と、前記受信した部分個人情報を出力する手段とを備えたことを特徴とする個人情報管理装置。

【請求項１６】　請求項１５の個人情報管理装置において、

前記個人情報利用者端末装置は、前記個人情報管理センタ装置から前記部分個人情報利用許諾情報に対して検索した部分個人情報の列の順序をランダムに入れ換えたものを受信する手段と、前記受信した部分個人情報の列を出力する手段とを備えたことを特徴とする個人情報管理装置。

【請求項１７】　請求項１６の個人情報管理装置において、

前記個人情報利用者端末装置は、利用しようとする部分個人情報に対応した部分個人情報利用許諾情報を取得する手段と、前記取得した部分個人情報利用許諾情報を前記個人情報管理センタ装置に送信する手段と、前記個人情報管理センタ装置が前記部分個人情報利用許諾情報に対して検証および該部分個人情報利用許諾情報に指定された個人情報を受信する手段と、前記受信した個人情報を復号する手段と、前記復号した部分個人情報を出力する手段とを備えたことを特徴とする個人情報管理装置。

【請求項１８】　請求項１７の個人情報管理装置におい

て、
前記個人情報利用者端末装置は、前記個人情報管理センタ装置が前記部分個人情報利用許諾情報に対して検証および該部分個人情報利用許諾情報に指定された個人情報を該個人情報管理センタ装置のみが知る鍵を用いて暗号化した提供者暗号化部分個人情報の列を受信する手段と、前記受信した提供者暗号化部分個人情報を復号する手段と、前記暗号化部分を個人情報利用者端末装置のみが知る鍵を用いて暗号化する手段と、前記暗号化した部分個人情報の列を前記個人情報管理センタ装置に送信する手段と、前記個人情報管理センタ装置が前記利用者暗号化センタ暗号化部分個人情報の列に含まれる利用者暗号化センタ暗号化部分個人情報を鍵を用いて復号し、部分個人情報の列の順序を入れ替えた利用者暗号化部分個人情報の列を受信する手段と、前記受信した利用者暗号化部分個人情報を復号する手段と、前記復号した部分個人情報を出力する手段とを備えたことを特徴とする個人情報管理装置。

【請求項１９】　個人情報提供者端末装置で提供する個人情報を通信手段を介して個人情報管理センタ装置に登録し、個人情報利用者端末装置が前記個人情報を通信手段を介して取得して利用する個人情報管理方法であって、
前記個人情報提供者端末装置は、入力された個人情報を単独では特定の個人との関連づけができずに意味をなさない部分個人情報に分割し、この部分個人情報を前記個人情報管理センタ装置に送信し、前記個人情報管理センタ装置で部分個人情報に対して生成した部分個人情報識別子を受信し、前記受信した部分個人情報識別子によって表される部分個人情報の内容と対応づけて保存し、提供しようとする部分個人情報に対応した部分個人情報識別子を前記個人情報関連記憶手段から取得して前記個人情報利用者端末装置に送信することを特徴とする個人情報管理方法。

【請求項２０】　個人情報提供者端末装置で提供する個人情報を通信手段を介して個人情報管理センタ装置に登録し、個人情報利用者端末装置が前記個人情報を通信手段を介して取得して利用する個人情報管理方法であって、
前記個人情報管理センタ装置は、個人情報をを単独では特定の個人との関連づけができずに意味をなさない部分個人情報に分割した部分個人情報を前記個人情報提供者端末装置から受信し、前記受信した部分個人情報に識別子を生成し、該生成した部分個人情報識別子と前記部分個人情報とを対応させて保存し、前記部分個人情報識別子を個人情報提供者端末装置に送信し、前記個人情報利用者端末装置から受信した部分個人情報識別子に対応する部分個人情報を前記部分個人情報記憶手段から検索し、前記検索された部分個人情報を前記個人情報提供者端末装置に送信することを特徴とする個人情報管理方法。

【請求項２１】　個人情報提供者端末装置で提供する個人情報を通信手段を介して個人情報管理センタ装置に登録し、個人情報利用者端末装置が前記個人情報を通信手段を介して取得して利用する個人情報管理方法であって、
前記個人情報利用者端末装置は、前記個人情報提供者端末装置から提供したい部分個人情報に対応した部分個人情報識別子を受信し、前記受信した個人情報識別子を部分個人情報識別子記憶装置に保存し、前記保存した部分個人情報識別子を前記個人情報管理センタ装置に送信し、前記送信に対して前記個人情報管理センタ装置から部分個人情報識別子に対応する部分個人情報を受信し、該受信した部分個人情報を出力することを特徴とする個人情報管理方法。

【請求項２２】請求項１～５、請求項１３～１８、請求項１９または２１のいずれか１項に記載の装置または方法における処理をコンピュータに実行させるためのプログラムを、該コンピュータが読み取り可能な記録媒体に記録したことを特徴とする個人情報管理装置または方法を実行するプログラムを記録した記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ネットワークを通じて利用者の嗜好などの個人情報を収集する際に、利用者が自分の個人情報の利用方法を制御可能にするための個人情報管理方法および個人情報管理装置に関するものである。

【０００２】

【従来の技術】近年、インターネットなどのネットワークの発展により、双方向の通信を利用した情報提供手段が利用できるようになり、利用者から提供される利用者個人の嗜好などの個人情報を収集し、個々人の嗜好に適した情報や広告を提供する情報提供サービスが盛んに利用されるようになってきた。

【０００３】例えば、利用者の嗜好に応じて利用者の興味のありそうな情報を電子メールを通じて利用者に届けたり、利用者がWWW（ＷｏｒｌｄＷｉｄｅＷｅｂ）のコンテンツを閲覧する際にユーザに適した広告を表示したりといったサービスが行なわれている。また、ネットワークを通じて商品の販売を行なう業者は、商品販売の際に商品の提供に必要な配送先などの個人情報を収集できれば効率よいな商取引が可能となる。

【０００４】

【発明が解決しようとする課題】上記のように、ネットワークの利用者が個人情報を提供する機会が増えているが、こういった個人情報の提供の際に人の手で逐一個人情報の入力と提供を行なっていては利便性が悪いため、個人情報を個人情報管理センタに集めておき、それを利用することが考えられるが、それでは利用者のプライバ

シを個人情報管理センタに把握されてしまう問題があった。

【０００５】また、このような目的で収集される個人情報は、一旦利用者が情報提供者に渡してしまえば、利用者はその情報の利用方法についてそれ以上制御することができなくなっていた。すなわち、情報提供者が収集した個人情報を利用者が同意した方法以外に利用したり、第三者に提供される恐れがある。

【０００６】このような課題を解決しようとする方式として、特開平９－９１３５８号公報、特開平１１－１４９５０４号公報、特開平１１－２７３６８１号公報に開示された技術がある。

【０００７】上記の特開平９－９１３５８号公報の技術は、情報提供者と受信者との間で送受信要件を通信し、双方の希望が満足される配信リストを生成する。しかし、第三者に対して送受信情報の開示を制限するものではないため、個人情報が第三者に提供される恐れがある。

【０００８】特開平１１－１４９５０４号公報の技術は、指定された参照者にのみ個人情報取得を許すものであるが、登録者から発行された問い合わせコードと参照者側からの応答との一致を確認してから参照者に個人情報を伝達する。しかし、送受信情報を判読不可能にするものではないため、情報漏れの恐れがある。

【０００９】特開平１１－２７３６８１号公報に技術は、許可されない参照者が個人情報を読み出しても解読不可能にすることを目的とする。そのために個人情報を基本情報ファイルと属性情報ファイルに分割し、暗号化コードで互いに関連付けるものである。しかし、分割情報（暗号化コード）の伝達経路や格納場所で情報が漏れる恐れがある。

【００１０】本発明の目的は、個人情報を提供することを許諾した者以外の、例えば個人情報の提供を仲介する個人情報管理センタにも個人情報の提供者のプライバシを把握されないようにした個人情報管理装置および個人情報管理方法を提供することにある。

【００１１】本発明の他の目的は、個人情報をその利用者に提供する際に、個人情報の利用方法に関し、個人情報の提供者が柔軟に制御ができるようにすること、特に、個人を特定できる形で情報を渡さずに、個人情報の統計的使用のみを許可できるようにする個人情報管理装置および個人情報管理方法を提供することにある。

【００１２】

【課題を解決するための手段】本発明では、個人情報を他者に提供しようとする個人情報提供者に関する個人情報を、それぞれ単独では特定の個人との関連づけができずに意味をなさない部分個人情報に分割した上で個人情報管理センタに登録し、それらの間の関連は個人情報提供者の持つ端末でのみ保持することで、個人情報管理センタでは個人情報提供者のプライバシを把握できなくする。

【００１３】また、個人情報提供者から個人情報提供者の個人情報を利用しようとする個人情報利用者に対しては、個人情報管理センタに登録された部分個人情報の識別子と、個人情報取得許諾条件をセットにして提供し、取得許諾条件に合う場合にのみ個人情報管理センタが部分個人情報を個人情報利用者に提供することで個人情報の利用方法をユーザが制御する。

【００１４】さらに、個人情報管理センタが個人情報利用者からの複数の取得要求を一括して受け付け、これに対する回答となる部分個人情報の順序をランダムに入れ換えて送信することで統計的利用に限った取得許諾を可能にする。

【００１５】以上のことから、本発明は、以下の個人情報管理方法、個人情報管理装置、及び個人情報管理装置または方法を実行するプログラムを記録する記録媒体を特徴とする。

【００１６】（個人情報提供者端末装置）個人情報提供者端末装置で提供する個人情報を通信手段を介して個人情報管理センタ装置に登録し、個人情報利用者端末装置が前記個人情報を通信手段を介して取得して利用する個人情報管理装置であって、前記個人情報提供者端末装置は、入力された個人情報を単独では特定の個人との関連づけができずに意味をなさない部分個人情報に分割するための個人情報分割手段と、この部分個人情報を前記個人情報管理センタ装置に送信する手段と、前記個人情報管理センタ装置で部分個人情報に対して生成した部分個人情報識別子を受信する手段と、前記受信した部分個人情報識別子によって表される部分個人情報の内容と対応づけて保存する部分個人情報関連記憶手段と、提供しようとする部分個人情報に対応した部分個人情報識別子を前記部分個人情報関連記憶手段から取得して前記個人情報利用者端末装置に送信する手段とを備えたことを特徴とする個人情報管理装置。

【００１７】また、前記個人情報提供者端末装置は、前記部分個人情報識別子を部分個人情報関連記憶手段から取り出して前記個人情報管理センタ装置に送信する手段と、前記個人情報管理センタ装置から部分個人情報識別子に対応する部分個人情報を受信する手段と、前記受信した前記部分個人情報を出力する手段を備えたことを特徴とする個人情報管理装置。

【００１８】また、前記個人情報提供者端末装置は、変更しようとする個人情報を入力する手段と、前記個人情報分割手段によって分割された部分個人情報の内容に応じた部分個人情報識別子を前記部分個人情報関連記憶手段から検索する手段と、前記部分個人情報とその識別子を対にして前記個人情報管理センタ装置に送信する手段とを備えたことを特徴とする個人情報管理装置。

【００１９】また、前記個人情報提供者端末装置は、前記部分個人情報関連記憶手段から提供したい部分個人情

報に対応した部分個人情報識別子を取り出す手段と、前記個人情報利用者端末装置にどのような部分個人情報をどのような条件で提供するのかを表す部分個人情報利用許諾情報を生成する手段と、前記個人情報利用者端末装置に対して前記部分個人情報利用許諾情報を送信する手段とを備えたことを特徴とする個人情報管理装置。

【００２０】また、前記個人情報提供者端末装置は、提供する個人情報を前記個人情報分割手段で分割した部分個人情報を暗号化するための暗号鍵を生成する手段と、各部分個人情報を前記暗号鍵を用いて暗号化する手段と、前記暗号化部分個人情報をそれぞれ別個に前記個人情報管理センタ装置に送信する手段と、前記個人情報管理センタ装置で生成し受信した部分個人情報識別子を、それによって表される部分個人情報の内容および、暗号化に用いた前記暗号化鍵と対応づけて前記部分個人情報関連記憶手段に保存する手段とを備えことを特徴とする個人情報管理装置。

【００２１】（個人情報管理センタ装置）個人情報提供者端末装置で提供する個人情報を通信手段を介して個人情報管理センタ装置に登録し、個人情報利用者端末装置が前記個人情報を通信手段を介して取得して利用する個人情報管理装置であって、前記個人情報管理センタ装置は、個人情報をを単独では特定の個人との関連づけができずに意味をなさない部分個人情報に分割した部分個人情報を前記個人情報提供者端末装置から受信する手段と、前記受信した部分個人情報に識別子を生成する識別子生成手段と、該生成した部分個人情報識別子と前記部分個人情報とを対応させて保存する部分個人情報記憶手段と、前記部分個人情報識別子を個人情報提供者端末装置に送信する手段と、前記個人情報利用者端末装置から受信した部分個人情報識別子に対応する部分個人情報を前記部分個人情報記憶手段から検索する手段と、前記検索された部分個人情報を前記個人情報提供者端末装置に送信する手段とを備えたことを特徴とする個人情報管理装置。

【００２２】また、前記個人情報管理センタ装置は、前記個人情報提供者端末装置が変更しようとする前記部分個人情報と該部分個人情報の内容に応じた部分個人情報識別子を受信する手段と、前記受信した部分個人情報識別子を用いて前記部分個人情報を検索してその値を受信した部分個人情報の値に変更する手段とを備えたことを特徴とする個人情報管理装置。

【００２３】また、前記個人情報管理センタ装置は、個人情報利用者端末装置が利用しようとする部分個人情報に対応した部分個人情報利用許諾情報を受信する手段と、前記受信した部分個人情報利用許諾情報が、当該個人情報利用者端末装置に対して、指定された部分個人情報の利用を許諾したものかどうかを検証する利用条件判断手段と、前記検証が成功した場合に前記部分個人情報利用許諾情報に指定された部分個人情報識別子に対応する部分個人情報を前記部分個人情報記憶手段から検索する手段と、前記検索した部分個人情報を前記個人情報利用者端末装置に送信する手段とを備えたことを特徴とする個人情報管理装置。

【００２４】また、前記個人情報管理センタ装置は、前記受信した部分個人情報利用許諾情報が条件を満たしていることを確認したときに該部分個人情報利用許諾情報に指定された部分個人情報識別子に対応する部分個人情報を前記部分個人情報記憶装置から検索する手段と、前記検索した部分個人情報の列の順序をランダムに入れ換える部分個人情報順序入換手段と、前記順序の入れ換えられた部分個人情報の列を前記個人情報利用者端末装置に送信する手段とを備えたことを特徴とする個人情報管理装置。

【００２５】また、前記個人情報管理センタ装置は、前記個人情報提供者端末装置が部分個人情報を暗号鍵を用いて暗号化した部分個人情報を受信する手段と、前記受信した暗号化部分個人情報に対応した部分個人情報識別子を生成する部分個人情報識別子生成手段と、前記生成した部分個人情報識別子と前記提供者暗号化部分個人情報とを対応させて前記部分個人情報記憶手段に保存する手段と、前記部分個人情報識別子を前記個人情報提供者端末装置に送信する手段とを備えたことを特徴とする個人情報管理装置。

【００２６】また、前記個人情報管理センタ装置は、前記個人情報利用者端末装置が利用しようとする部分個人情報に対応した部分個人情報利用許諾情報を受信する手段と、前記受信した部分個人情報利用許諾情報が、当該個人情報利用者端末装置に対して、指定された部分個人情報の利用を許諾したものかどうかを検証する利用条件判断手段と、前記検証が成功した場合に前記部分個人情報利用許諾情報に指定された部分個人情報識別子に対応する部分個人情報を前記部分個人情報記憶手段から検索する手段と、前記検索した部分個人情報を前記個人情報利用者端末装置に送信する手段とを備えたことを特徴とする個人情報管理装置。

【００２７】また、前記個人情報管理センタ装置は、前記部分個人情報利用許諾情報に指定された部分個人情報識別子に対応する部分個人情報を前記部分個人情報記憶装置から検索する手段と、各提供者暗号化部分個人情報を個人情報管理センタ装置のみが知る鍵を用いて暗号化してセンタ暗号化提供者暗号化部分個人情報の列を得て前記個人情報利用者端末装置に送信する手段と、前記個人情報利用者端末装置から受信した前記利用者暗号化センタ暗号化部分個人情報の列に含まれる利用者暗号化センタ暗号化部分個人情報をそれぞれ鍵を用いて復号する手段と、前記復号した利用者暗号化部分個人情報の列の順序をランダムに入れ換える部分個人情報順序入換手段と、前記入れ換えた利用者暗号化部分個人情報の列を前記個人情報利用者端末装置に送信する手段とを備えたこ

とを特徴とする個人情報管理装置。

【００２８】（個人情報利用者端末装置）個人情報提供者端末装置で提供する個人情報を通信手段を介して個人情報管理センタ装置に登録し、個人情報利用者端末装置が前記個人情報を通信手段を介して取得して利用する個人情報管理装置であって、前記個人情報利用者端末装置は、前記個人情報提供者端末装置から提供したい部分個人情報に対応した部分個人情報識別子を受信する手段と、前記受信した個人情報識別子を部分個人情報識別子記憶装置に保存する手段と、前記保存した部分個人情報識別子を前記個人情報管理センタ装置に送信する手段と、前記送信に対して前記個人情報管理センタ装置から部分個人情報識別子に対応する部分個人情報を受信する手段と、該受信した部分個人情報を出力する手段とを備えたことを特徴とする個人情報管理装置。

【００２９】また、前記個人情報利用者端末装置は、前記個人情報提供者端末装置から提供したい部分個人情報についてどのような部分個人情報をどのような条件で提供するのかを表す部分個人情報利用許諾情報を受信する手段と、前記受信した部分個人情報利用許諾情報を部分個人情報利用許諾情報記憶手段に保存することを特徴とする個人情報管理装置。

【００３０】また、前記個人情報利用者端末装置は、利用したい部分個人情報に対応した部分個人情報利用許諾情報を前記部分個人情報利用許諾情報記憶手段から取り出す手段と、該取り出した前記部分個人情報利用許諾情報を前記個人情報管理センタ装置に送信する手段と、前記部分個人情報利用許諾情報に対して個人情報管理センタ装置報により指定された部分個人情報の利用を許諾したことを検証し、該部分個人情報利用許諾情報に指定された部分個人情報識別子に対応する部分個人情報を受信する手段と、前記受信した部分個人情報を出力する手段とを備えたことを特徴とする個人情報管理装置。

【００３１】また、前記個人情報利用者端末装置は、前記個人情報管理センタ装置から前記部分個人情報利用許諾情報に対して検索した部分個人情報の列の順序をランダムに入れ換えたものを受信する手段と、前記受信した部分個人情報の列を出力する手段とを備えたことを特徴とする個人情報管理装置。

【００３２】また、前記個人情報利用者端末装置は、利用しようとする部分個人情報に対応した部分個人情報利用許諾情報を取得する手段と、前記取得した部分個人情報利用許諾情報を前記個人情報管理センタ装置に送信する手段と、前記個人情報管理センタ装置が前記部分個人情報利用許諾情報に対して検証および該部分個人情報利用許諾情報に指定された個人情報を受信する手段と、前記受信した個人情報を復号する手段と、前記復号した部分個人情報を出力する手段とを備えたことを特徴とする個人情報管理装置。

【００３３】また、前記個人情報利用者端末装置は、前記個人情報管理センタ装置が前記部分個人情報利用許諾情報に対して検証および該部分個人情報利用許諾情報に指定された個人情報を該個人情報管理センタ装置のみが知る鍵を用いて暗号化した提供者暗号化部分個人情報の列を受信する手段と、前記受信した提供者暗号化部分個人情報を復号する手段と、前記暗号化部分を個人情報利用者端末装置のみが知る鍵を用いて暗号化する手段と、前記暗号化した部分個人情報の列を前記個人情報管理センタ装置に送信する手段と、前記個人情報管理センタ装置が前記利用者暗号化センタ暗号化部分個人情報の列に含まれる利用者暗号化センタ暗号化部分個人情報を鍵を用いて復号し、部分個人情報の列の順序を入れ替えた利用者暗号化部分個人情報の列を受信する手段と、前記受信した利用者暗号化部分個人情報を復号する手段と、前記復号した部分個人情報を出力する手段とを備えたことを特徴とする個人情報管理装置。

【００３４】（個人情報管理方法）個人情報提供者端末装置で提供する個人情報を通信手段を介して個人情報管理センタ装置に登録し、個人情報利用者端末装置が前記個人情報を通信手段を介して取得して利用する個人情報管理方法であって、前記個人情報提供者端末装置は、入力された個人情報を単独では特定の個人との関連づけができずに意味をなさない部分個人情報に分割し、この部分個人情報を前記個人情報管理センタ装置に送信し、前記個人情報管理センタ装置で部分個人情報に対して生成した部分個人情報識別子を受信し、前記受信した部分個人情報識別子によって表される部分個人情報の内容と対応づけて保存し、提供しようとする部分個人情報に対応した部分個人情報識別子を前記個人情報関連記憶手段から取得して前記個人情報利用者端末装置に送信することを特徴とする個人情報管理方法。

【００３５】個人情報提供者端末装置で提供する個人情報を通信手段を介して個人情報管理センタ装置に登録し、個人情報利用者端末装置が前記個人情報を通信手段を介して取得して利用する個人情報管理方法であって、前記個人情報管理センタ装置は、個人情報をを単独では特定の個人との関連づけができずに意味をなさない部分個人情報に分割した部分個人情報を前記個人情報提供者端末装置から受信し、前記受信した部分個人情報に識別子を生成し、該生成した部分個人情報識別子と前記部分個人情報とを対応させて保存し、前記部分個人情報識別子を個人情報提供者端末装置に送信し、前記個人情報利用者端末装置から受信した部分個人情報識別子に対応する部分個人情報を前記部分個人情報記憶手段から検索し、前記検索された部分個人情報を前記個人情報提供者端末装置に送信することを特徴とする個人情報管理方法。

【００３６】個人情報提供者端末装置で提供する個人情報を通信手段を介して個人情報管理センタ装置に登録し、個人情報利用者端末装置が前記個人情報を通信手段

を介して取得して利用する個人情報管理方法であって、前記個人情報利用者端末装置は、前記個人情報提供者端末装置から提供したい部分個人情報に対応した部分個人情報識別子を受信し、前記受信した個人情報識別子を部分個人情報識別子記憶装置に保存し、前記保存した部分個人情報識別子を前記個人情報管理センタ装置に送信し、前記送信に対して前記個人情報管理センタ装置から部分個人情報識別子に対応する部分個人情報を受信し、該受信した部分個人情報を出力することを特徴とする個人情報管理方法。

【００３７】（記録媒体）前記の装置または方法における処理をコンピュータに実行させるためのプログラムを、該コンピュータが読み取り可能な記録媒体に記録したことを特徴とする個人情報管理装置または方法を実行するプログラムを記録した記録媒体。

【００３８】

【発明の実施の形態】（実施形態１）個人情報の管理委託

本実施形態は、次のように実施することで、個人情報提供者のプライバシを知られることなしに、個人情報提供者の個人情報の管理を個人情報管理センタに任せることにより、個人情報を保存しておくには十分な容量を持たない個人情報提供者端末装置を用いて、個人情報提供者の個人情報を参照することができるようにするものであり、以下に詳細に説明する。

【００３９】（システム構成）図１は、本実施形態を示すシステム構成図である。システムは、個人情報を提供する側のユーザが利用する個人情報提供者端末装置１０１と、個人情報提供者端末装置１０１から受け取った個人情報を管理し、個人情報提供者端末装置１０１の必要に応じて個人情報を送信する個人情報管理センタ装置１０２とから構成される。各装置は互いにネットワークを通じて通信するものとする。

【００４０】なお、個人情報提供者端末装置１０１と個人情報管理センタ装置１０２との間の通信は、個人情報管理センタ装置１０２から見て通信をしている個人情報提供者端末装置１０１を特定できないような匿名通信路を用いて行なってもよい。

【００４１】（各装置の構成）図２に個人情報提供者端末装置１０１の構成を示す。個人情報提供者端末装置１０１は、個人情報管理センタ装置１０２と通信するための通信機能２０１と、個人情報を入力するための個人情報入力機能２０２と、個人情報を個々の部分に分割するための個人情報分割機能２０３と、部分に分けられて個人情報管理センタ装置１０２に送信した個人情報の関連と意味を保存する部分個人情報関達ＤＢ（データベース）２０４と、個人情報管理センタ装置１０２から送られた個人情報を出力する個人情報出力機能２０５とから構成される。

【００４２】図３に個人情報管理センタ装置１０２の構成を示す。個人情報管理センタ装置１０２は、個人情報提供者端末装置１０１と通信するための通信機能３０１と、部分個人情報識別子を生成する部分個人情報識別子生成機能３０２と、分割された個々の個人情報を保存する部分個人情報ＤＢ３０３とから構成される。

【００４３】（処理の概要）本実施形態の処理は、個人情報提供者端末装置１０１が個人情報管理センタ装置１０２に対して個人情報を登録する個人情報登録処理と、個人情報提供者端末装置１０１が個人情報管理センタ装置１０２から登録済みの個人情報を取得する個人情報取得処理とから構成される。

【００４４】（個人情報登録）図４に個人情報の登録処理の流れを示す。まずステップ４０１において、個人情報提供者端末装置１０１は個人情報を提供する者の個人情報を入力する。ここで個人情報とは、例えばその提供者の氏名、郵便番号、住所、年齢、性別などの他、趣味、好きな音楽のジャンル、髪の色、身長、体重など、上記提供者の特徴を表すどのような情報でもよい。ここでは一つの例として図１７のような情報が入力されたものとする。

【００４５】ステップ４０２において、個人情報分割機能７０３によって、入力された個人情報を、それぞれ単独では特定の個人との関連づけができずに意味をなさない部分個人情報に分割する。このような分割方法として、例えば、図１８に示すように、上記の名前～趣味までの情報をそれぞれ別個の部分個人情報となるように分割してもよい。この場合、“Ａｌｉｃｅ”，“１１１”などの部分個人情報を単独で与えても、Ａｌｉｃｅという人物がどのような人物であるかを知ることはできない。これらの部分個人情報は、“Ａｌｉｃｅ”がその人物の名前であり、“１１１”がその人物の住所の郵便番号であり、“１－１　Ｓｏｕｔｈｅｒｎ　Ａｖｅ”がその人物の住所であり……といった事実、すなわち、これらの部分個人情報がその特定の人物によって結びつけられているという部分個人情報間の関連を知らなければ意味をなさない。

【００４６】あるいは、図１９に示すように、より細かく文字を単位に分割してもよい。この場合、“Ａ”がその人物の名前の一文字目であり、“ｌ”がその人物の名前の二文字目であり、……という部分個人情報間の関連を知ることがなければ“Ａｌｉｃｅ”という単語すら知られることはない。

【００４７】さらに、個人情報をビット列で表し、それを前から順に適当なビット数ずつ切り出したものを部分個人情報としてもよい。例えば、“Ａｌｉｃｅ…”を01000,00101,10100,10110,00110,11001,01…とする。

【００４８】ただし、これらの分割方法は、本発明の請求範囲を限定するものではなく、入力された個人情報をそれぞれ単独では特定の個人との関連づけができずに、意味をなさない部分個人情報に分割する方法であれば、

どのような方法を用いても構わない。

【００４９】ステップ４０３において、個人情報提供者端末装置１０１は、上記部分個人情報をそれぞれ別個に個人情報管理センタ装置１０２に送信する。例えば“Ａｌｉｃｅ”を送信したとする。

【００５０】ステップ４０４において、個人情報管理センタ装置１０２は、部分個人情報識別子生成機能８０２によって受信した部分個人情報に対応した識別子（部分個人情報識別子）を生成する。ここで、個人情報管理センタ装置１０２がシステム内に複数存在する場合には、個人情報管理センタ装置１０２を特定する個人情報管理センタ識別子が上記部分個人情報識別子に含まれるようにしてもよい。

【００５１】ステップ４０５において、生成した上記部分個人情報識別子と上記部分個人情報とを対応させて部分個人情報ＤＢ３０３に保存する。図１０に部分個人情報ＤＢの構成例を示す。ただし、図１０は部分個人情報ＤＢの構成を限定するものではなく、部分個人情報識別子と部分個人情報の対応関係を保持できるものであればどのような構成であってもよい。

【００５２】ステップ４０６において、個人情報管理センタ装置１０２は上記部分個人情報識別子を個人情報提供者に送信する。

【００５３】ステップ４０７において、個人情報提供者端末装置は上記部分個人情報識別子を、それによって表される部分個人情報の内容と対応づけて部分個人情報関連ＤＢ２０４に保存する。このとき、個人情報管理センタ装置１０２に送信した部分個人情報の値とも関連づけて保存してもよい。図１１に部分個人情報関連ＤＢ２０４の構成例を示す。ただし、図１１は部分個人情報関連ＤＢ２０４の構成を限定するものではなく、部分個人情報識別子と部分個人情報の内容の対応関係を保持できるものであればどのような構成であってもよい。

【００５４】ステップ４０２で分割した全ての部分個人情報に対して、ステップ４０３からステップ４０６までの処理を繰り返す。個人情報管理センタ装置が複数ある場合には、それぞれの部分個人情報を異なる個人情報管理センタ装置に送信してもよい。

【００５５】個人情報提供者端末装置１０１と個人情報管理センタ装置１０２の間の通信が匿名通信路を介して行なわれる場合には、個人情報管理センタ装置１０２は個々の部分個人情報が同一の個人情報提供者によるものであることが分からないため、個人情報管理センタ装置１０２は個人情報提供者のプライバシを知ることがない。個人情報管理センタ装置１０２が、個々の部分個人情報が関連するものであることを推測できないようにするために、各部分個人情報に対するステップ４０３からステップ４０６までの処理を連続して行なわずに、適宜時間間隔をおいて処理してもよい。

【００５６】このようにして、例えば、部分個人情報関連ＤＢ３０３には図２０に示すような情報が保存される。ここで、id_1～id_6は部分個人情報識別子である。また、例えば部分個人情報関連ＤＢ２０４には図２１に示すような情報が保存される。

【００５７】（個人情報取得）図５に個人情報の取得処理の流れを示す。まず、ステップ５０１において、個人情報提供者端末装置１０１は、利用したい部分個人情報の内容に対応した部分個人情報識別子を部分個人情報関連ＤＢ２０４から取り出す。

【００５８】ステップ５０２において個人情報利用者端末装置１０１から個人情報管理センタ装置１０２に対し、上記部分個人情報識別子を送信する。個人情報管理センタ装置が複数存在する場合には、上記部分個人情報識別子に含まれる個人情報管理センタ識別子を利用して個人情報管理センタ装置を特定する。

【００５９】ステップ５０３において、個人情報管理センタ装置１０２は、受信した部分個人情報識別子に対応する部分個人情報を、部分個人情報ＤＢ３０３から検索する。

【００６０】ステップ５０４において、個人情報管理センタ装置１０２から個人情報提供者端末装置１０１に対し、検索された上記部分個人情報を送信する。

【００６１】ステップ５０５において、個人情報提供者端末装置１０１は受信した上記部分個人情報を出力する。

【００６２】（実施形態１のまとめ）以上のような手順を用いて、個人情報提供者の個人情報を個人情報管理センタ装置において管理することで、個人情報管理センタ装置に保存されている情報を見てもれぞれの部分個人情報同士の関連が分からないため、個人情報管理センタ装置からＤＢのデータが漏洩しても個人情報提供者のプライバシが守られる。

【００６３】また、個人情報提供者端末装置と個人情報管理センタ装置との間の通信が匿名通信路を介して行なわれれば、個人情報管理センタ装置も、部分個人情報同士の関連を知ることが不可能となり、個人情報提供者のプライバシを守るのに好適となる。

【００６４】（実施形態２）個人情報提供の基本形

本実施形態は、個人情報提供者の個人情報を分割した部分個人情報を個別に個人情報管理センタ装置１０２に保存し、ユーザ端末装置においてそれら部分個人情報間の関連づけを保存するためのものであり、以下に詳細に説明する。

【００６５】（システム構成）図６は、本発明の実施形態を示すシステム構成図である。システムは、個人情報を提供する側のユーザが利用する個人情報提供者端末装置６０１と、個人情報を利用する側である個人情報利用者端末装置６０２と、個人情報提供者端末装置６０１から受け取った個人情報を管理し、個人情報利用者端末装置６０２に個人情報を必要に応じて提供する個人情報管

理センタ装置６０３とから構成される。

【００６６】各装置は互いにネットワークを通じて通信するものとする。システム内には個々の個人情報の提供者および個人情報の利用者に対応した、それぞれ複数の個人情報提供者端末装置、個人情報利用者端末装置があってもよい。あるいは、複数の個人情報管理センタ装置があってもよい。

【００６７】具体的には、例えば、個人情報利用者端末装置６０２は、ネットワーク上でコンテンツを販売し、コンテンツの購入者の嗜好情報を集計して商品のマーケティングに利用したいと考えるコンテンツ販売業者によって利用される。一方、個人情報提供者端末装置６０１は、上記コンテンツ販売業者からコンテンツを購入するユーザによって利用されていてもよい。ただし、この具体例は本発明の請求範囲を限定するものではない。

【００６８】なお、個人情報提供者端末装置６０１と個人情報管理センタ装置６０３との間の通信は、個人情報管理センタ装置６０３から見て通信をしている個人情報提供者端末装置６０１を特定できないような匿名通信路を用いて行なってもよい。

【００６９】（各装置の構成）図７に個人情報提供者端末装置６０１の構成を示す。個人情報提供者端末装置６０１は、個人情報管理センタ装置６０３および個人情報利用者端末装置６０２と通信するための通信機能７０１と、個人情報を入力するための個人情報入力機能７０２と、個人情報を個々の部分に分割するための個人情報分割機能７０３と、部分に分けられて個人情報管理センタ装置６０３に送信した個人情報の関連と意味を保存する部分個人情報関連ＤＢ７０４とから構成される。

【００７０】図８に個人情報管理センタ装置６０３の構成を示す。個人情報管理センタ装置６０３は、個人情報提供者端末装置６０１および個人情報利用者端末装置６０２と通信するための通信機能８０１と、部分個人情報識別子を生成する部分個人情報識別子生成機能８０２と、分割された個々の個人情報を保存する部分個人情報ＤＢ８０３とから構成される。

【００７１】図９に個人情報利用者端末装置６０２の構成を示す。個人情報利用者端末装置６０２は、個人情報提供者端末装置６０１および個人情報管理センタ装置６０３と通信するための通信機能９０１と、個人情報管理センタ装置から送られた個人情報を出力する個人情報出力機能９０２と、個人情報提供者端末装置６０１から送られた、個人情報管理センタ装置６０３に対して個人情報を問い合わせる際に利用する部分個人情報識別子を保存する部分個人情報識別子ＤＢ９０３とから構成される。

【００７２】（処理の概要）図１３にシステム内で行なわれる処理の全体的な概要を示す。まず、ステップ１３０１で個人情報提供者端末装置６０１から個人情報提供者の個人情報を個人情報管理センタ装置６０３に送信し、個人情報管理センタ装置６０３に上記個人情報を登録する。

【００７３】次に、ステップ１３０２で個人情報提供者端末装置６０１から個人情報利用者端末装置６０２に対し、個人情報管理センタ装置６０３に登録された個人情報を識別するための情報を提供する。

【００７４】最後に、ステップ１３０３で個人情報利用者端末装置６０２が個人情報管理センタ装置６０３から登録された個人情報を取得する。

【００７５】（個人情報登録）図１４に個人情報の登録処理の流れを示す。まず、ステップ１４０１において、個人情報提供者端末装置６０１は個人情報を提供する者の個人情報を入力する。ここで、個人情報とは、例えばその提供者の氏名、郵便番号、住所、年齢、性別などの他、趣味、好きな音楽のジャンル、髪の色、身長、体重など、上記提供者の特徴を表すどのような情報でもよい。ここでは一つの例として図１７のような情報が入力されたものとする。

【００７６】ステップ１４０２において、個人情報分割機能７０３によって、入力された個人情報を、それぞれ単独では特定の個人との関連づけができずに意味をなさない部分個人情報に分割する。このような分割方法として、例えば、図１８に示すように、上記の名前～趣味までの情報をそれぞれ別個の部分個人情報となるように分割すること、あるいは、図１９に示すように文字を単位に分割するなど、前記のステップ４０２による分割と同様のものでよい。

【００７７】ステップ１４０３において、個人情報提供者端末装置６０１は、上記部分個人情報をそれぞれ別個に個人情報管理センタ装置６０３に送信する。例えば“ＡＩｉｃｅ”を送信したとする。

【００７８】ステップ１４０４において、個人情報管理センタ装置６０３は、部分個人情報識別子生成機能８０２によって受信した部分個人情報に対応した識別子（部分個人情報識別子）を生成する。ここで、個人情報管理センタ装置がシステム内に複数存在する場合には、個人情報管理センタ装置を特定する個人情報管理センタ識別子が上記部分個人情報識別子に含まれるようにしてもよい。

【００７９】ステップ１４０５において、生成した上記部分個人情報識別子と上記部分個人情報とを対応させて部分個人情報ＤＢ８０３に保存する。図１０に部分個人情報ＤＢの構成例を示す。ただし、図１０は部分個人情報ＤＢの構成を限定するものではなく、部分個人情報識別子と部分個人情報の対応関係を保持できるものであればどのような構成であってもよい。

【００８０】ステップ１４０６において、個人情報管理センタ装置６０３は上記部分個人情報識別子を個人情報提供者に送信する。

【００８１】ステップ１４０７において、個人情報提供

者は上記部分個人情報識別子を、それによって表される部分個人情報の内容と対応づけて部分個人情報関連ＤＢに保存する。このとき、個人情報管理センタ装置６０３に送信した部分個人情報の値とも関連づけて保存してもよい。図１１に部分個人情報関連ＤＢの構成例を示す。ただし、図１１は部分個人情報ＤＢの構成を限定するものではなく、部分個人情報識別子と部分個人情報の内容の対応関係を保持できるものであればどのような構成であってもよい。

【００８２】ステップ１４０２で分割した全ての部分個人情報に対して、ステツプ１４０３からステツプ１４０６までの処理を繰り返す。

【００８３】個人情報管理センタ装置が複数ある場合には、それぞれの部分個人情報を異なる個人情報管理センタ装置に送信してもよい。また、個人情報提供者端末装置と個人情報管理センタ装置の間の通信が匿名通信路を介して行なわれる場合には、個人情報管理センタ装置は個々の部分個人情報．が同一の個人情報提供者によるものであることが分からないため、個人情報管理センタ装置は個人情報提供者のプライバシを知ることがない。また、個人情報管理センタ装置が、個々の部分個人情報が関連するものであることを推測できないようにするために、各部分個人情報に対するステップ１４０３からステップ１４０６までの処理を連続して行なわずに、適宜時間間隔をおいて処理してもよい。

【００８４】このようにして、例えば、部分個人情報ＤＢ８０３には図２０に示すような情報が保存される。ここで、id_1～id_6は部分個人情報識別子である。

【００８５】また、例えば部分個人情報関連ＤＢ７０４には図２１に示すような情報が保存される。

【００８６】（個人情報提供）図１５に個人情報の提供処理の流れを示す。このような個人情報の提供処理は、具体的には例えば、コンテンツ販売業者がコンテンツを販売する際に、コンテンツの購入者から購入者の嗜好を取得したいような場合に、コンテンツ販売業者の利用する個人情報利用者端末から、上記購入者の利用する個人情報提供者端末に対して個人情報の提供を要求した場合などに行なわれる。ただし，この具体例は本発明の請求範囲を限定するものではない。

【００８７】まず、ステップ１５０１において、個人情報提供者端末装置６０１は、部分個人情報関連ＤＢ７０４から提供したい部分個人情報に対応した部分個人情報識別子を取り出す。

【００８８】ステップ１５０２において、個人情報提供者端末装置６０１から個人情報利用者端末装置６０２に対し、上記個人情報識別子を送信する。

【００８９】ステップ１５０３において、個人情報利用者端末装置６０２は、受信した個人情報識別子を、部分個人情報識別子ＤＢ９０３に保存する。このとき、上記個人情報識別子を、上記個人情報提供者端末装置６０１を利用する個人情報提供者と関連づけて保存してもよい。

【００９０】ステップ１５０２において、個人情報提供者が提供しようとする複数の部分個人情報に対応する部分個人情報識別子を同時に送信し、ステップ１５０３において上記部分個人情報識別子を互いに関連づけて保存してもよい。あるいは個人情報提供者が提供しようとする複数の部分個人情報毎にステップ１５０２からステップ１５０３を繰り返してもよい。

【００９１】図１２に部分個人情報識別子ＤＢの構成例を示す。ただし、図１２は部分個人情報識別子ＤＢの構成を限定するものではなく、部分個人情報識別子と個人情報提供者との関連を、個人情報の利用者の必要に応じて適宜保持するものであればどのような構成であってもよい。

【００９２】（個人情報取得）図１６に個人情報の取得処理の流れを示す。まず、ステップ１６０１において、個人情報利用者端末装置６０２は、利用したい部分個人情報に対応した部分個人情報識別子を部分個人情報識別子ＤＢ９０３から取り出す。

【００９３】ステップ１６０２において個人情報利用者端末装置６０２から個人情報管理センタ装置に対し、上記部分個人情報識別子を送信する。個人情報管理センタ装置が複数存在する場合には、上記部分個人情報識別子に含まれる個人情報管理センタ識別子を利用して個人情報管理センタ装置を特定する。

【００９４】ステップ１６０３において、個人情報管理センタ装置６０３は、受信した部分個人情報識別子に対応する部分個人情報を、部分個人情報ＤＢ８０３から検索する。

【００９５】ステップ１６０４において、個人情報管理センタ装置６０３から個人情報利用者端末装置６０２に対し、検索された上記部分個人情報を送信する。

【００９６】ステップ１６０５において、個人情報利用者端末装置６０２は受信した上記部分個人情報を出力する。

【００９７】（実施形態２のまとめ）以上のような手順を用いて、個人情報提供者から個人情報利用者に対して個人情報を提供することで、個人情報管理センタ装置に保存されている情報を見てもそれぞれの部分個人情報同士の関連が分からないため、個人情報管理センタ装置からＤＢのデータが漏洩しても個人情報提供者のプライバシが守られる。

【００９８】また、個人情報提供者端末装置と個人情報管理センタ装置との間の通信が匿名通信路を介して行なわれれば、個人情報管理センタ装置も、部分個人情報同士の関連を知ることが不可能となり、個人情報提供者のプライバシが守られる。

【００９９】（実施形態３）個人情報の変更

本実施形態は、実施形態２で示したシステムにおいて、

個人情報提供者が一旦個人情報管理センタ装置に登録した個人情報を変更するためのものであり、以下に詳細に説明する。

【０１００】（個人情報の変更）図２２に個人情報の変更処理の流れを示す。まず、ステップ２２０１において、個人情報提供者端末装置は、変更しようとする個人情報を入力する。

【０１０１】ステップ２２０２において、個人情報分割機能によって、入力された個人情報を、それぞれ単独では特定の個人との関連づけができずに意味をなさない部分個人情報に分割する。この分割は、実施形態２におけるステップ１４０２と同様のものである。

【０１０２】ステップ２２０３において、分割されたそれぞれの上記部分個人情報の内容に応じた部分個人情報識別子を、部分個人情報関連ＤＢ７０４から検索する。

【０１０３】ステップ２２０４において、個人情報提供者端末装置６０１から個人情報管理センタ装置６０３に対し、入力され分割されたた上記部分個人と、検索された上記部分個人情報識別子とを対にして送信する。

【０１０４】ステップ２２０５において、個人情報管理センタ装置６０３は、部分個人情報ＤＢ８０３から受信した部分個人情報識別子を用いて検索し、対応する部分個人情報の値を受信した部分個人情報の値と置き換える。

【０１０５】ここで、ステップ２２０１からステップ２２０４において個人情報を新たに入力して送信する代わりに、部分個人情報識別子を、部分個人情報を消去するような指示とともに個人情報管理センタ装置６０３に送信することで、個人情報管理センタ装置６０３に登録された部分個人情報を消去し、以降個人情報利用者端末装置６０２からの個人情報取得要求に応えないようにすることもできる。

【０１０６】また、部分個人情報を変更する個人情報提供者端末装置が、確かに指定された部分個人情報識別子に対応する部分個人情報を登録した個人情報提供者端末装置であるかどうかを認証を行なってもよい。例えば、個人情報の登録処理において、個々の部分個人情報毎に匿名公開鍵を生成し、個人情報の変更処理時に、対応する秘密鍵を用いることで認証を行なってもよい。その場合には、例えば、部分個人情報ＤＢ８０３の１エントリ毎に匿名公開鍵の項を追加し、部分個人情報関連ＤＢ７０４の１エントリ毎に匿名公開鍵および秘密鍵の対の項を追加する。

【０１０７】図２３、図２４にそれぞれこの例の場合の部分個人情報ＤＢ８０３および部分個人情報関連ＤＢ７０４の構成例を示す。ただし、図２３および図２４は部分個人情報ＤＢおよび部分個人情報関連ＤＢの構成を限定するものではない。

【０１０８】この認証は、部分個人情報を変更する個人情報提供者端末装置が、確かに指定された部分個人情報識別子に対応する部分個人情報を登録した個人情報提供者端末装置であることを確かめられる認証方式であればどのような方式を用いてもよい。また、個人情報管理センタ装置が、複数の部分個人情報が同一の個人情報提供者端末装置から登録されたものであることを知ることができないように、個別の部分個人情報に対して個別の認証を行なうようにしてもよい。例えば、部分個人情報識別子の発行毎にパスワードを設定し、そのパスワードを用いて認証してもよい。

【０１０９】（実施形態３のまとめ）以上のような手順を用いて、個人情報管理センタ装置に登録された個人情報を変更、あるいは消去することで、個人情報利用者端末装置が個人情報取得要求によって取得する個人情報を、個人情報提供者が必要に応じて制御することが可能となる。

【０１１０】具体的には、例えば、実施形態２で示した具体例において、Ａｌｉｃｅが転居して住所が変更になった場合に、ステップ２２０４において（ｃ、“２－２ＮｏｒｔｈｅｒｎＡｖｅ．”）を送信することで、それ以降個人情報利用者端末装置が取得する個人情報の、住所の情報を変更することができる。

【０１１１】（実施形態４）部分個人情報利用許諾情報本実施形態は、個人情報提供者から個人情報利用者に対して部分個人情報識別子を提供する際に、その部分個人情報の利用に関する制限条件を課すものである。

【０１１２】本実施形態においては、実施形態２における個人情報管理センタ装置６０３を、図２５のように構成する。ここで、個人情報管理センタ装置６０３は、個人情報提供者端末装置６０１および個人情報利用者端末装置６０２と通信するための通信機能２５０１と、部分個人情報識別子を生成する部分個人情報識別子生成機能２５０２と、分割された個々の個人情報を保存する部分個人情報ＤＢ２５０４と、部分個人情報に関する利用条件を判断する利用条件判断機能２５０３から構成される。

【０１１３】一方、個人情報利用者端末装置６０２は、図９における部分個人情報識別子ＤＢ９０３の代わりに部分個人情報利用許諾情報ＤＢを持つ。

【０１１４】（個人情報提供）実施形態２において図１５に示した個人情報提供処理の代わりに、図２６に示す処理を行なう。

【０１１５】図２６のステップ２６０１においては、個人情報提供者端末装置６０１は、部分個人情報関連ＤＢ７０４から提供したい部分個人情報に対応した部分個人情報識別子を取り出す。

【０１１６】ステップ２６０２において、個人情報利用者端末装置６０２にどのような部分個人情報をどのような条件で提供するのかを表す部分個人情報利用許諾情報を生成する。このような部分個人情報利用許諾情報としては、例えば図２８のような構成の情報を用いても良

い。

【０１１７】この部分個人情報利用許諾情報は、図２８の個人情報利用者識別子２８０１で示される個人情報利用者は、部分個人情報識別子２８０３で示される部分個人情報を、個人情報利用条件２８０２で示される利用条件下であれば、部分個人情報管理センタから取得して利用することができることを表す。

【０１１８】ここで、部分個人情報識別子２８０３は、単一の部分個人情報識別子であってもよいし、複数の部分個人情報識別子の列であってもよい。後者の場合には、上記部分個人情報識別子の列に含まれる各部分個人情報識別子に対応する部分個人情報全体に対して個人情報利用条件が適用されることを表す。

【０１１９】ステップ２６０３において、個人情報提供者端末装置６０１から個人情報利用者端末装置６０２に対し、上記部分個人情報利用許諾情報を送信する。

【０１２０】ステップ２６０４において、個人情報利用者端末装置６０２は、受信した上記部分個人情報利用許諾情報を部分個人情報利用許諾情報ＤＢに保存する。

【０１２１】（個人情報取得）実施形態２において図１６に示した個人情報取得処理の代わりに、図２７に示した処理を行なう。

【０１２２】まず、ステップ２７０１において、個人情報利用者端末装置６０２は、利用したい部分個人情報に対応した部分個人情報利用許諾情報を部分個人情報利用許諾情報ＤＢから取り出す。

【０１２３】ステップ２７０２において、個人情報利用者端末装置６０２から個人情報管理センタ装置６０３に対し、上記部分個人情報利用許諾情報を送信する。

【０１２４】ステップ２７０３において、個人情報管理センタ装置６０３は、利用条件判断機能によって、受信した上記部分個人情報利用許諾情報が、確かに通信している個人情報利用者端末装置６０２に対して、指定された部分個人情報の利用を許諾したものかどうかを検証する。

【０１２５】上記検証が成功した場合、ステップ２７０４において、個人情報管理センタ装置６０３は、上記部分個人情報利用許諾情報に指定された部分個人情報識別子に対応する部分個人情報を、部分個人情報ＤＢ８０３から検索する。

【０１２６】ステップ２７０５において、個人情報管理センタ装置６０３から個人情報利用者端末装置６０１に対し、検索された上記部分個人情報を送信する。

【０１２７】ステップ２７０６において、個人情報利用者端末装置６０２は受信した上記部分個人情報を出力する。

【０１２８】上記ステップ２７０３における検証は、部分個人情報利用許諾情報の構成に応じて、その利用許諾を確かに検証できる方法であればどのようなものであってもよい。例えば、上記部分個人情報利用許諾情報が図２８のように構成されている場合には、まず通信をしている個人情報利用者端末装置が、個人情報利用者識別子２８０１によって示されるものであるかどうかを検証する。さらに、個人情報利用条件２８０２が満たされているかどうかを検証する。

【０１２９】（個人情報利用条件の定義）図２８の個人情報利用条件２８０２としては、例えば、部分個人情報を取得することのできる期限を定めてもよい。また、部分個人情報の利用目的を限定してもよい。さらに、一定数以上の部分個人情報の取得を同時に行なわなければならないとしてもよい。さらにまた、部分個人情報に対して何らかの演算を加えた上で、個人情報管理センタ装置から個人情報利用者端末装置へ部分個人情報を送信することを条件とするなどの部分個人情報の提供の形態に関する条件を定めても良い。もしくは、個人情報管理センタ装置から個人情報利用者端末装置に部分個人情報を送信する際に、一旦他の何らかの装置を経由してから送信するなどの部分個人情報の提供の方式に関する条件を定めてもよい。

【０１３０】ただし、これらの例は個人情報利用条件の内容を限定するものではなく、個人情報の提供および利用に関する条件であって、個人情報管理センタが検証可能なものであればどのような条件であってもよい。

【０１３１】（部分個人情報利用許諾情報の間接的提供）個人情報提供者端末装置６０１は、ステップ２６０３において、個人情報利用者識別子２８０１で示された個人情報利用者端末に直接部分個人情報利用許諾情報を送信しなくても良い。

【０１３２】具体的には、例えば、コンテンツの配送を行なう業者の個人情報利用者識別子とコンテンツの配送先を表す部分個人情報に対応した部分個人情報識別子を指定した部分個人情報利用許諾情報を、コンテンツ購入要求とともにコンテンツの販売を行なう業者に対して送信し、上記販売業者が上記配送業者に対し、要求されたコンテンツとともに上記部分個人情報利用許諾情報を送信することで、上記配送業者のみがコンテンツの配送に必要な個人情報を取得できるようにしてもよい。ただし、この具体例は上記のような部分個人情報利用許諾情報の間接的提供の実施形態を限定するものではない。

【０１３３】（部分個人情報利用許諾情報への署名）部分個人情報利用許諾情報を、確かに個人情報提供者端末装置がステップ２６０２において生成したものであり、個人情報利用者端末装置あるいはその他の者が偽造したものではないことを、個人情報管理センタがステップ２７０３において検証してもよい。

【０１３４】例えば、個人情報の登録処理において、個々の部分個人情報毎に匿名公開鍵を生成し、対応する秘密鍵で、部分個人情報利用許諾情報に部分個人情報提供者端末装置の電子署名を加えても良い。その場合、部分個人情報ＤＢ２５０４の１エントリごとに匿名公開鍵の

項を追加し、部分個人情報関連ＤＢ７０４の１エントリ毎に匿名公開鍵／秘密鍵のペアの項を追加する。ステップ２７０３における個人情報利用条件の判断の際には、部分個人情報識別子から対応する匿名公開鍵を調べ、これを用いて署名を検証することで、それが正しく上記個人情報提供者端末装置によって生成されたものであることを検証してもよい。あるいはこれ以外の方法を用いて上記検証を行なっても良い。

【０１３５】（実施形態５）統計的利用

本実施形態は、個人情報利用条件として、「ｎ個以上の部分個人情報全体としての統計的利用であること」という条件を用いた場合である。

【０１３６】本実施形態においては、実施形態４における個人情報管理センタ装置６０３を、図２９のように構成する。ここで、個人情報管理センタ装置６０３は、個人情報提供者端末装置６０１および個人情報利用者端末装置６０２と通信するための通信機能２９０１と、部分個人情報識別子を生成する部分個人情報識別子生成機能２９０２と、分割された個々の個人情報を保存する部分個人情報ＤＢ２９０５と、部分個人情報に関する利用条件を判断する利用条件判断機能２５０３とに加え、部分個人情報の列を個人情報利用者端末装置に送信する前に順序を入れ換える部分個人情報順序入換機能２９０４とから構成される。

【０１３７】（個人情報取得）図３０に、個人情報取得処理の流れを示す。まず、ステップ３００１において、個人情報利用者端末装置６０２は、利用したい部分個人情報に対応した部分個人情報利用許諾情報を部分個人情報識別子ＤＢ９０３から取り出す。このとき、個人情報利用条件を満たすため、必要な数ｎ個以上の部分個人情報利用許諾情報を取りだし、部分個人情報利用許諾情報の列とする。

【０１３８】ステップ３００２において、個人情報利用者端末装置６０２から個人情報管理センタ装置６０３に対し、上記部分個人情報利用許諾情報の列を送信する。

【０１３９】ステップ３００３において、個人情報管理センタ装置６０３は、利用条件判断機能によって、受信した上記部分個人情報利用許諾情報が、確かに通信している個人情報利用者端末装置に対して、指定された部分個人情報の利用を許諾したものかどうかを検証する。この中では同時に取得すべき部分個人情報の数ｎについても検証が行なわれる。このとき、部分個人情報利用許諾情報の列に含まれるすべての部分個人情報利用許諾情報が条件を満たしていることを確認する。

【０１４０】上記検証が成功した場合、ステップ３００４において、個人情報管理センタ装置６０３は、上記部分個人情報利用許諾情報に指定された部分個人情報識別子に対応する部分個人情報を、部分個人情報ＤＢ８０３から検索し、部分個人情報の列とする。

【０１４１】ステップ３００５において、部分個人情報

順序入換機能２９０４を用いて、上記部分個人情報の列の順序をランダムに入れ換える。

【０１４２】ステップ３００６において、個人情報管理センタ装置６０３から個人情報利用者端末装置６０２に対し、順序の入れ換えられた上記部分個人情報の列を送信する。

【０１４３】ステップ３００７において、個人情報利用者端末装置６０２は受信した上記部分個人情報の列を出力する。

【０１４４】個人情報利用者端末装置６０２は、順序を入れ換えられた部分個人情報を取得するため、個々の部分個人情報利用許諾情報が、どの部分個人情報に対応しているのかを知ることはなく、特定の個人に関する情報を入手することはできない。一方で、複数の部分個人情報全体として、例えば部分個人情報の値の平均値や、分布を求めるなどの統計処理に利用することが可能である。

【０１４５】具体的には、コンテンツの販売業者が、本実施形態での個人情報利用者端末装置を利用することで、コンテンツ購入者の個々の嗜好情報を入手することなしに、コンテンツ購入者の嗜好の傾向を統計的に入手することができる。ただし、この具体例は、本発明の適用範囲を限定するものではない。

【０１４６】（実施形態６）部分個人情報の暗号化

本実施形態は、個人情報管理センタ装置６０３に登録する部分個人情報を、個人情報提供者端末装置６０１で暗号化してから個人情報管理センタ装置に送信するものである。

【０１４７】本実施形態においては、個人情報提供者端末装置６０１は、実施形態２における図７の構成に加え、部分個人情報を暗号化するための暗号化機能を持つ。

【０１４８】また、個人情報利用者端末装置６０２は、実施形態２における図９あるいは実施形態４における個人情報利用者端末装置の構成に加え、暗号化された部分個人情報を復号するための復号機能を持つ。

【０１４９】（個人情報登録）図３１に、個人情報登録処理の流れを示す。まず、ステップ３１０１において、個人情報提供者端末装置６０２は個人情報を提供する者の個人情報を入力する。ここで個人情報とは、例えばその提供者の氏名、郵便番号、住所、年齢、性別などの他、趣味、好きな音楽のジャンル、髪の色、身長、体重など、上記提供者の特徴を表すどのような情報でもよい。ここでは一つの例として図１７のような情報が入力されたものとする。

【０１５０】ステップ３１０２において、個人情報分割機能７０３によって、入力された個人情報を、それぞれ単独では特定の個人との関連づけができずに意味をなさない部分個人情報に分割する。このような分割方法として、例えば、図１８に示すように、上記の名前～趣味ま

での情報をそれぞれ別個の部分個人情報となるように分割してもよい。あるいは、図１９に示すように文字を単位に分割してもよい。

【０１５１】ステップ３１０３において、個人情報提供者端末装置６０１は、部分個人情報を暗号化するための暗号鍵を生成する。登録する部分個人情報全体で共通の暗号鍵を利用してもよいが、それぞれの部分個人情報ごとにことなる暗号鍵を生成してもよい。

【０１５２】ステップ３１０４において、それぞれの部分個人情報を暗号鍵を用いて暗号化する。例えば図３３のような提供者暗号化部分個人情報を得る。ここで、E_{k1}～E_{k6}は、それぞれ暗号鍵k_1～k_6による暗号化関数を表す。

【０１５３】ステップ３１０５において、個人情報提供者端末装置６０１は、上記提供者暗号化部分個人情報をそれぞれ別個に個人情報管理センタ装置６０３に送信する。例えば“E_{k1}（Ａｌｉｃｅ）”を送信したとする。

【０１５４】ステップ３１０６において、個人情報管理センタ装置６０３は、部分個人情報識別子生成機能８０２によって受信した暗号化部分個人情報に対応した識別子（部分個人情報識別子）を生成する。

【０１５５】ステップ３１０７において、生成した上記部分個人情報識別子と上記提供者暗号化部分個人情報とを対応させて部分個人情報ＤＢ８０３に保存する。部分個人情報ＤＢは実施形態２の部分個人情報ＤＢと同様の構成であってよい。

【０１５６】ステップ３１０８において、個人情報管理センタ装置６０３は上記部分個人情報識別子を個人情報提供者に送信する。

【０１５７】ステップ３１０９において、個人情報提供者は上記部分個人情報識別子を、それによって表される部分個人情報の内容および、暗号化に用いた暗号化鍵と対応づけて部分個人情報関連ＤＢ７０４に保存する。このとき、個人情報管理センタに送信した部分個人情報の値とも関連づけて保存してもよい。

【０１５８】ステップ３１０２で分割した全ての部分個人情報に対して、ステップ３１０５からステップ１４０６までの処理を繰り返す。

【０１５９】したがって、部分個人情報を暗号化して送信するため、個人情報提供者端末装置６０１と個人情報管理センタ装置６０３の間の通信が、匿名通信路を介して行なわれなくても、個人情報提供者のプライバシが知られずに済む。

【０１６０】（個人情報提供）個人情報提供の際には、部分個人情報利用許諾情報に加え、その部分個人情報の暗号化に用いた暗号鍵を、個人情報提供者端末装置６０１から個人情報利用者端末装置６０２に送信する。個人情報利用者端末装置６０２は、受信した部分個人情報利用許諾情報と上記暗号鍵とを関連づけて部分個人情報利用許諾情報ＤＢに保存する。

【０１６１】（個人情報取得）図３２に個人情報取得処理の流れを示す。この処理では、図２７に示す実施形態４の個人情報取得処理において、部分個人情報の代わりに提供者暗号化部分個人情報を、個人情報管理センタ装置から個人情報利用者端末装置に送信し、さらに、個人情報利用者端末装置が、上記提供者暗号化部分個人情報を復号するステップ３２０６が加わっている。

【０１６２】（実施形態７）暗号化と順序入換えの個人情報取得

本実施形態は、実施形態６の部分個人情報の暗号化を行なった上で、実施形態５と同様の部分個人情報の順序入換えを行なうものである。

【０１６３】本実施形態においては、個人情報管理センタ装置６０３は、実施形態５の図２９の構成に加え、部分個人情報の暗号化／復号機能を持つ。また、個人情報利用者端末装置６０２は実施形態６の個人情報利用者端末装置の構成に加え、部分個人情報の暗号化機能を持つ。

【０１６４】また、個人情報提供者端末装置６０１および個人情報管理センタ装置６０３および個人情報利用者端末装置６０２が備える暗号化機能は、暗号化とは異なる順序で復号しても復号が可能な、順序の可換な暗号化を行なうものとする。

【０１６５】図３４に、個人情報取得処理の流れを示す。ステップ３４０１からステップ３４０４までは、部分個人情報が暗号化されて提供者暗号化部分個人情報となっている以外は、図３０のステップ３００１からステップ３００４までと同様である。

【０１６６】ステップ３４０５において、個人情報管理センタ装置６０３は、各提供者暗号化部分個人情報を個人情報管理センタ装置のみが知る鍵を用いて暗号化してセンタ暗号化提供者暗号化部分個人情報の列を得る。

【０１６７】ステップ３４０６において、個人情報管理センタ装置６０３から個人情報利用者端末装置６０２に対して上記センタ暗号化提供者暗号化部分個人情報の列を送信する。

【０１６８】ステップ３４０７において、個人情報利用者端末装置６０２は、上記センタ暗号化提供者暗号化部分個人情報の列に含まれるセンタ暗号化提供者暗号化部分個人情報をそれぞれ部分個人情報利用許諾情報に関連づけられた暗号鍵で復号し、センタ暗号化部分個人情報の列を得る。

【０１６９】ステップ３４０８において、個人情報利用者端末装置６０２は、上記センタ暗号化部分個人情報の列に含まれるセンタ暗号化部分個人情報を個人情報利用者端末装置のみが知る鍵を用いて暗号化して、利用者暗号化センタ暗号化部分個人情報の列を得る。

【０１７０】ステップ３４０９において、個人情報利用者端末装置６０２から個人情報管理センタ装置６０３に対して上記利用者暗号化センタ暗号化部分個人情報の列

を送信する。

【０１７１】ステップ３４１０において、個人情報管理センタ装置６０３は、上記利用者暗号化センタ暗号化部分個人情報の列に含まれる利用者暗号化センタ暗号化部分個人情報をそれぞれ上記個人情報管理センタ装置のみが知る鍵を用いて復号して利用者暗号化部分個人情報の列を得る。

【０１７２】ステップ３４１１において、部分個人情報順序入換機能を用いて、上記利用者暗号化部分個人情報の列の順序をランダムに入れ換える。

【０１７３】ステップ３４１２において、個人情報管理センタ装置６０３から個人情報利用者端末装置６０２に対し、順序の入れ換えられた上記利用者暗号化部分個人情報の列を送信する。

【０１７４】ステップ３４１３において、個人情報利用者端末装置６０２は受信した上記利用者暗号化部分個人情報の列を上記個人情報利用者端末装置のみが知る鍵を用いて復号し、部分個人情報の列を得る。

【０１７５】ステップ３４１４において、個人情報利用者端末装置６０２は上記部分個人情報の列を出力する。

【０１７６】上記個人情報管理センタ装置６０３のみが知る鍵は、常に同じ鍵を用いても、毎回異なる鍵を用いても良い。上記個人情報利用者端末装置のみが知る鍵は、同時に取得する部分個人情報の列全体に対して同一の鍵を用いていれば、常に同じ鍵を用いても、毎回異なる鍵を用いても良い。

【０１７７】なお、本発明の個人情報管理装置または方法における図４等の手順図で示した各実施形態例での処理の手順ないし計算アルゴリズムをコンピュータ等に実行させるためのプログラムを該コンピュータが読み取り可能な記録媒体、例えばフロッピー（登録商標）ディスクやメモリカード、ＭＯ、ＣＤ、ＤＶＤなどに記録して配布することが可能である。

【０１７８】

【発明の効果】以上のとおり、本発明によれば、以下の効果がある。

【０１７９】（１）（個人情報の分割）本発明は、個人情報提供者の個人情報を登録する個人情報管理センタ装置の持つデータベースの内容が万が一外部に漏洩することがあっても、個人情報提供者のプライバシが知られることがない。

【０１８０】（２）（匿名で登録）本発明は、個人情報提供者の個人情報を登録する個人情報管理センタ装置においても、個人情報提供者のプライバシが知られることがない。

【０１８１】（３）（識別子を渡す）本発明は、個人情報提供者のプライバシを守った状態で、必要な個人情報に限り、個人情報利用者に対して個人情報を提供することができ、また、個人情報利用者が取得する個人情報の内容を、個人情報提供者が後から変更することができる。

【０１８２】（４）（個人情報取得許諾条件の利用）本発明は、不当な個人情報利用者が、あるいは不当な方法で個人情報提供者の個人情報を利用することを制限し、個人情報の利用を個人情報提供者が制御することができる。

【０１８３】（５）（統計的利用のみ）本発明は、個人情報利用者が、統計的な利用方法でのみ個人情報を利用し、特定の個人情報提供者の個人情報が把握されることがない。

【０１８４】（６）（部分個人情報の暗号化）本発明は、匿名通信路を利用することなしに、個人情報提供者の個人情報を登録する個人情報管理センタ装置においても、個人情報提供者のプライバシが知られることがない。

【０１８５】（７）（全体）本発明は、個人情報提供者の個人情報を登録する個人情報管理センタ装置に個人情報提供者のプライバシが知られるなど、個人情報提供者以外の者に個人情報提供者のプライバシが知られることなしに、個人情報提供者が許諾した個人情報利用者が、個人情報提供者の許諾した方法で個人情報を利用するように個人情報提供者が制御することができる。また、個人情報提供者が、個人情報利用者に対し、個人情報の統計的利用のみを許諾することができる。

【図面の簡単な説明】

【図１】システムの全体構成を表す。

【図２】個人情報提供者端末装置の構成を表す。

【図３】個人情報管理センタ装置の構成を表す。

【図４】個人情報登録処理のフローを表す。

【図５】個人情報取得処理のフローを表す。

【図６】システムの全体構成を表す。

【図７】個人情報提供者端末装置の構成を表す。

【図８】個人情報管理センタ装置の構成を表す。

【図９】個人情報利用者端末装置の構成を表す。

【図１０】部分個人情報ＤＢの構成例を表す。

【図１１】部分個人情報関連ＤＢの構成例を表す。

【図１２】部分個人情報識別子ＤＢの構成例を表す。

【図１３】全体的な処理の概要を表す。

【図１４】個人情報登録処理のフローを表す。

【図１５】個人情報提供処理のフローを表す。

【図１６】個人情報取得処理のフローを表す。

【図１７】入力される個人情報の例を表す。

【図１８】部分個人情報への分割の一つ目の例を表す。

【図１９】部分個人情報への分割の二つ目の例を表す。

【図２０】部分個人情報ＤＢへ保存されるデータの例を表す。

【図２１】部分個人情報関連ＤＢへ保存されるデータの例を表す。

【図２２】個人情報変更処理のフローを表す。

【図２３】部分個人情報ＤＢの構成例を表す。

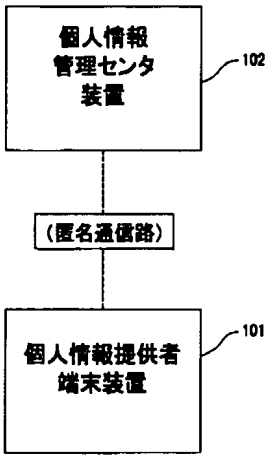
31

【図２４】部分個人情報関連ＤＢの構成例を表す。
【図２５】個人情報管理センタ装置の構成を表す。
【図２６】個人情報提供処理のフローを表す。
【図２７】個人情報取得処理のフローを表す。
【図２８】部分個人情報利用許諾情報の構成例を表す。
【図２９】個人情報管理センタ装置の構成を表す。
【図３０】個人情報取得処理のフローを表す。
【図３１】個人情報登録処理のフローを表す。
【図３２】個人情報取得処理のフローを表す。
【図３３】暗号化された部分個人情報の例を表す。
【図３４】個人情報取得処理のフローを表す。
【符号の説明】
１０１、６０１…個人情報提供者端末装置

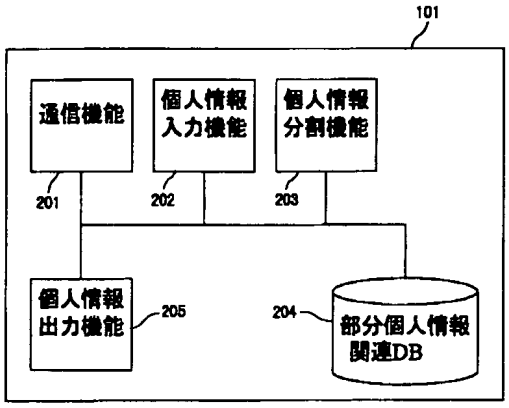
32

１０２、６０３…個人情報管理センタ装置
６０２…個人情報利用者端末装置
２０２…個人情報入力機能
２０３、７０３…個人情報分割機能
２０４、７０４…部分個人情報関連ＤＢ
３０２、８０２、２５０２、２９０２…部分個人情報識別子生成機能
３０３、８０３、２５０４、２９０５…部分個人情報ＤＢ
９０３…部分個人情報識別子ＤＢ
２５０３…利用条件判断機能
２９０４…部分個人情報順序入換機能

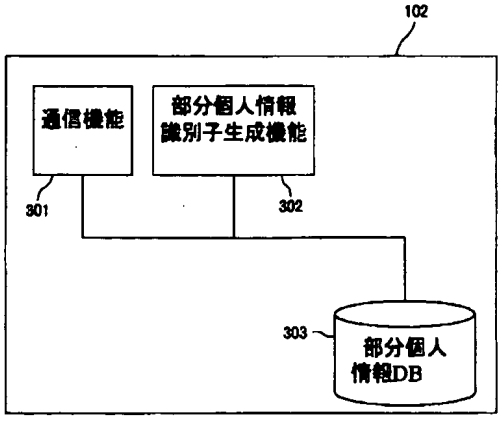
【図１】



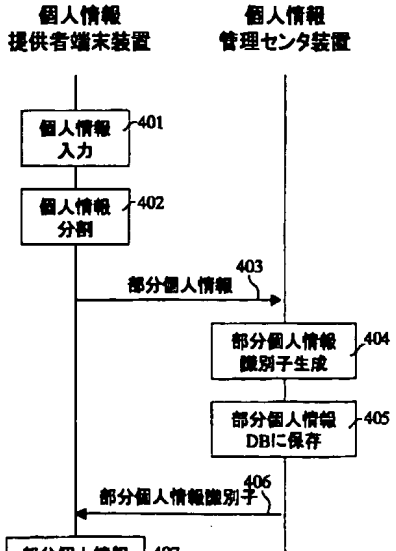
【図２】



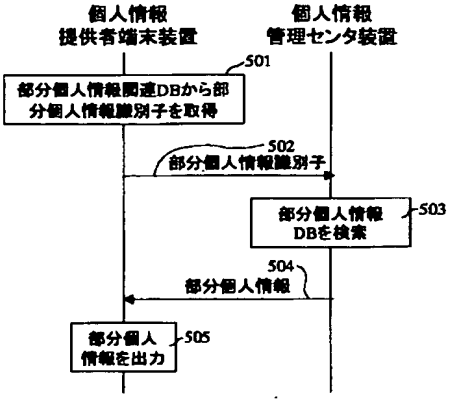
【図３】



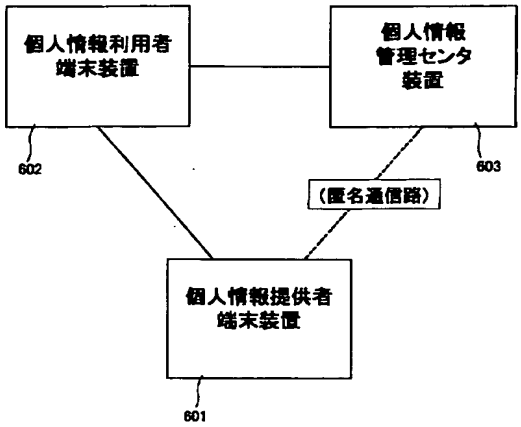
【図４】



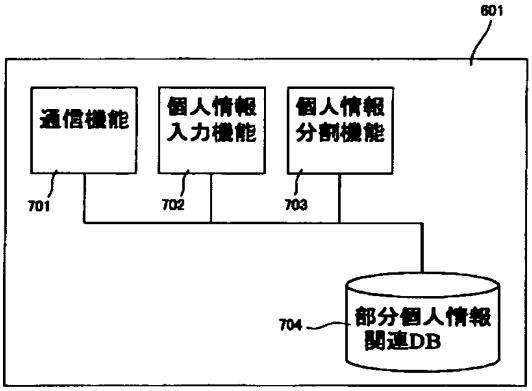
【図５】



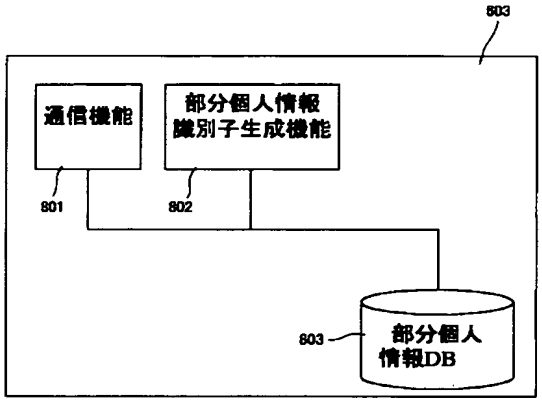
【図６】



【図７】



【図８】



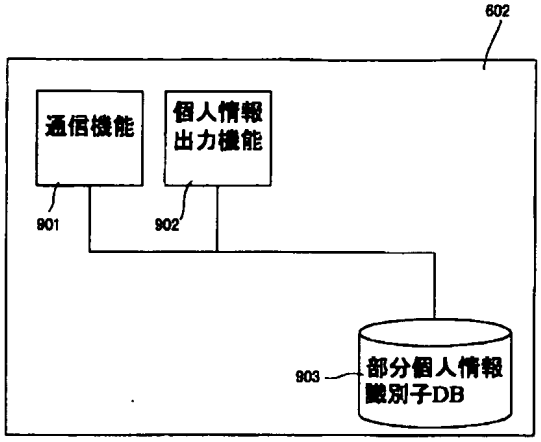
【図１０】

部分個人情報識別子	部分個人情報
id_1	Alice
id_2	1-1 Southern Ave.

【図１１】

部分個人情報識別子	内容
id_1	氏名
id_2	郵便番号
id_3	住所
id_4	年齢
:	:
:	:

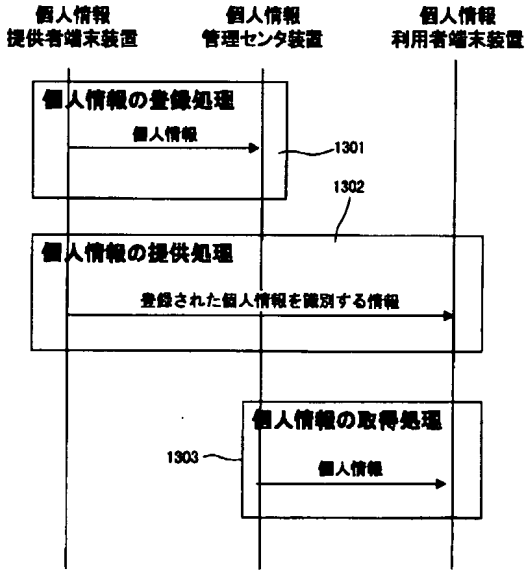
【図９】



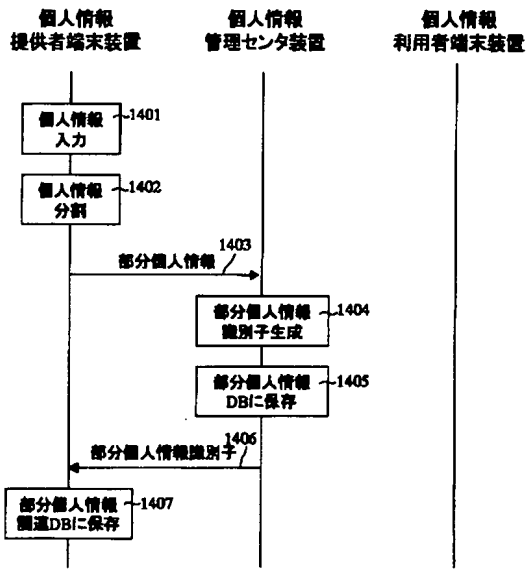
【図１２】

No.	名前	趣味	. . .
1	id_1	id_3	
2	id_2	id_4	. . .
:	:	:	

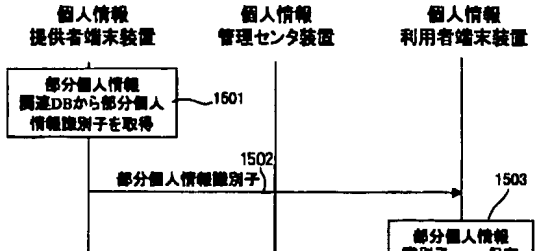
【図１３】



【図１４】



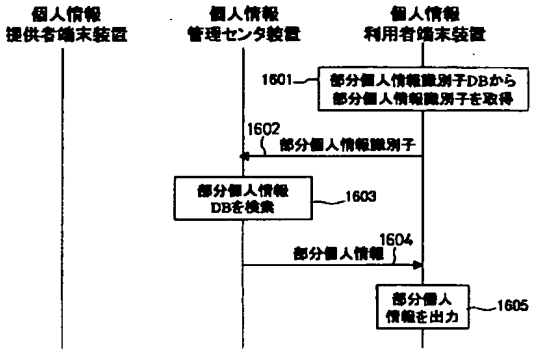
【図１５】



【図１７】

名前	Alice
郵便番号	111
住所	1-1 Southern Ave.
年齢	24
性別	female
趣味	music

【図１６】



【図１８】

部分個人情報1	Alice
部分個人情報2	111
部分個人情報3	1-1 Southern Ave.
部分個人情報4	24
部分個人情報5	female
部分個人情報6	music

【図１９】

部分個人情報1	A
部分個人情報2	l
部分個人情報3	i
部分個人情報4	c
部分個人情報5	e
部分個人情報6	1
⋮	⋮

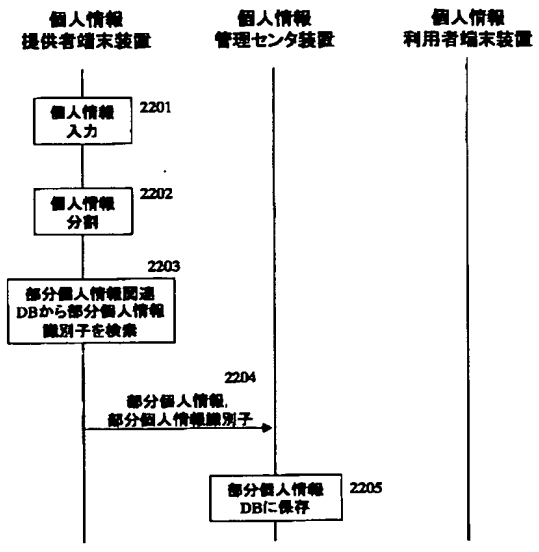
【図２０】

部分個人情報識別子	部分個人情報
id_1	Alice
id_2	111
id_3	1-1 Southern Ave.
id_4	24
id_5	female
id_6	music

【図２１】

部分個人情報識別子	内容
id_1	名前
id_2	郵便番号
id_3	住所
id_4	年齢
id_5	性別
id_6	趣味

【図２２】



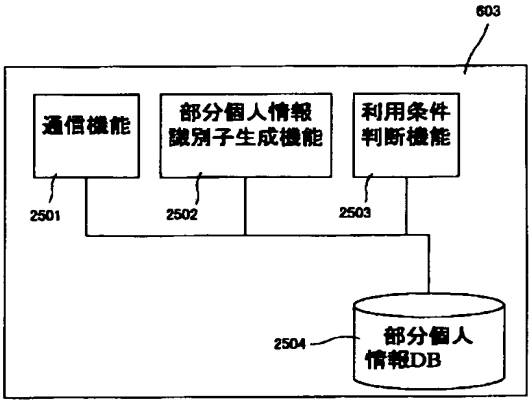
【図２３】

匿名公開鍵	部分個人情報識別子	部分個人情報
Pa	id_1	Alice
Pb	id_2	111
Pc	id_3	1-1 Southern Ave.
Pd	id_4	24
:	:	:
:	:	:

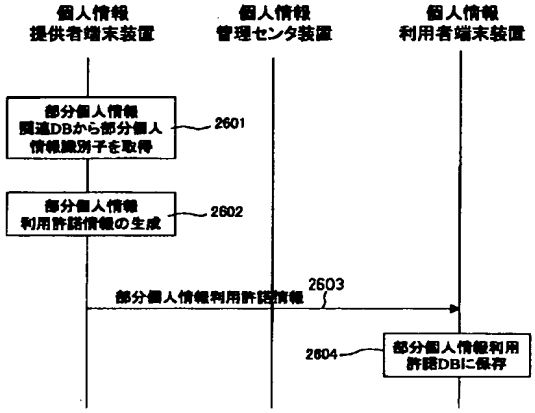
【図２４】

匿名公開鍵・秘密鍵	部分個人情報識別子	内容
Pa, Sa	id_1	氏名
Pb, Sb	id_2	郵便番号
Pc, Sc	id_3	住所
Pd, Sd	id_4	年齢
:	:	:
:	:	:

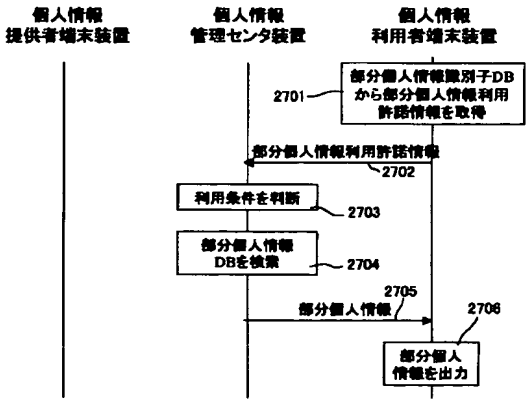
【図２５】



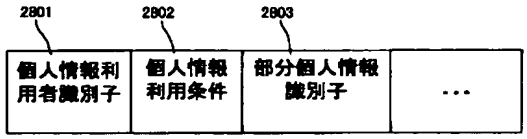
【図２６】



【図２７】



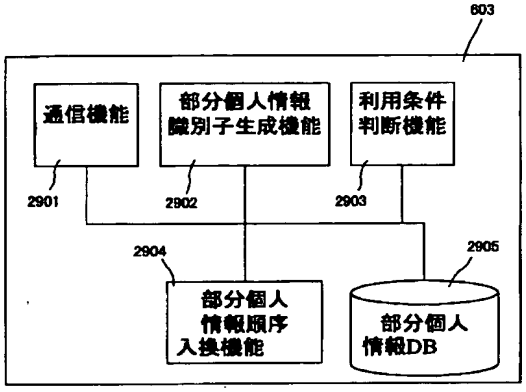
【図２８】



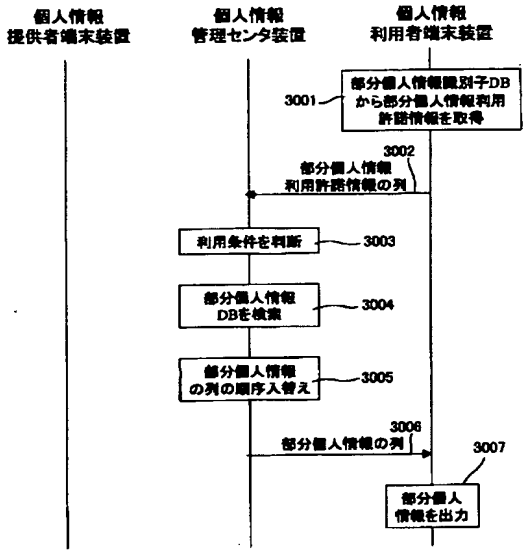
【図３３】

提供者暗号化部分個人情報1	E_{k1}(Alice)
提供者暗号化部分個人情報2	E_{k2}(111)
提供者暗号化部分個人情報3	E_{k3}(1-1 Southern Ave.)
提供者暗号化部分個人情報4	E_{k4}(24)
提供者暗号化部分個人情報5	E_{k5}(female)
提供者暗号化部分個人情報6	E_{k6}(music)

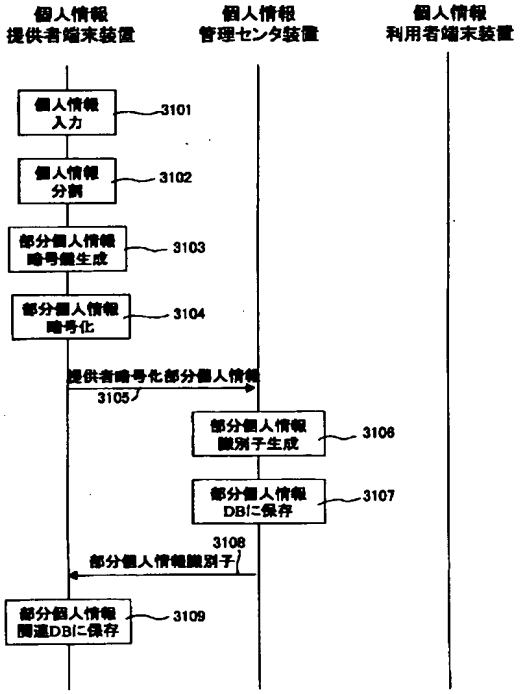
【図２９】



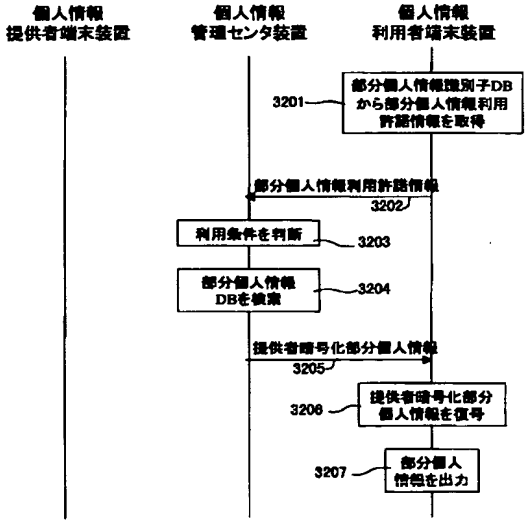
【図３０】



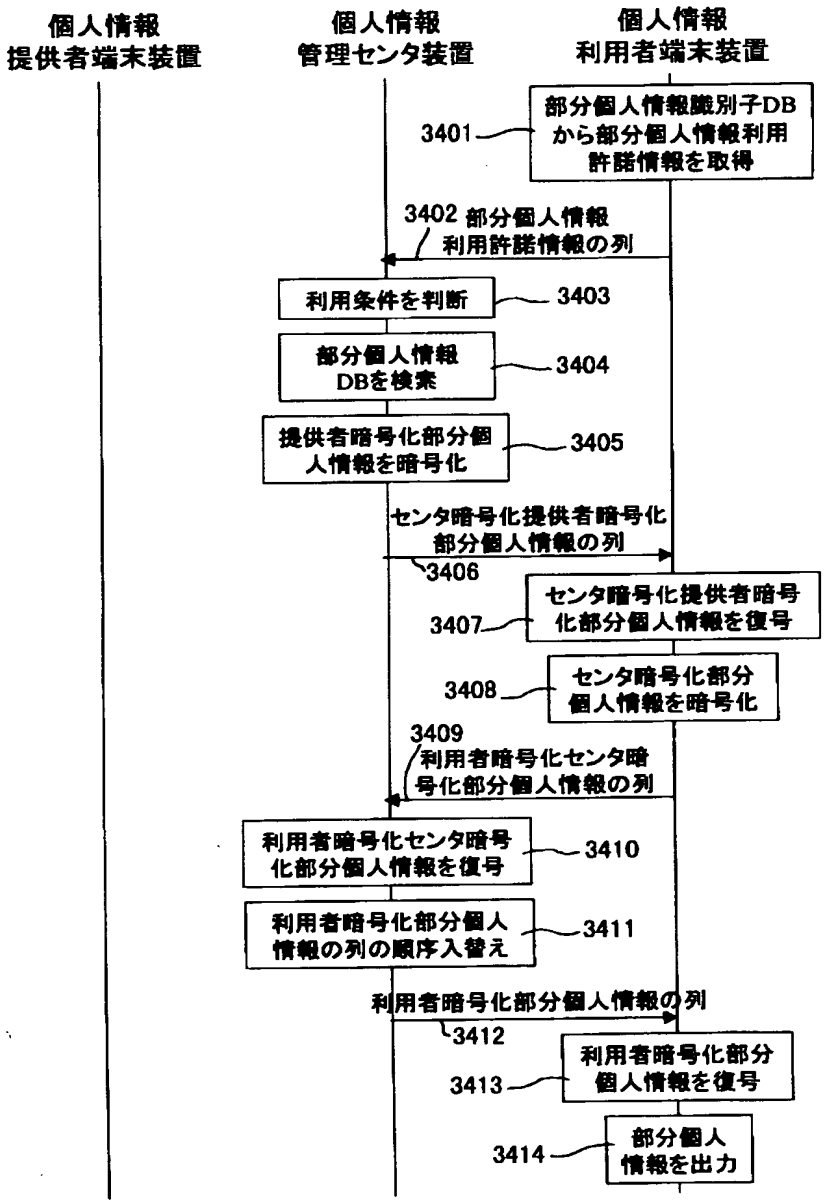
【図３１】



【図３２】



【図３４】


個人情報
提供者端末装置
個人情報
管理センタ装置
個人情報
利用者端末装置
3401
部分個人情報識別子DBから部分個人情報利用許諾情報を取得
3402 部分個人情報利用許諾情報の列
利用条件を判断
3403
部分個人情報DBを検索
3404
提供者暗号化部分個人情報を暗号化
3405
センタ暗号化提供者暗号化部分個人情報の列
3406
3407
センタ暗号化提供者暗号化部分個人情報を復号
3408
センタ暗号化部分個人情報を暗号化
3409
利用者暗号化センタ暗号化部分個人情報の列
利用者暗号化センタ暗号化部分個人情報を復号
3410
利用者暗号化部分個人情報の列の順序入替え
3411
利用者暗号化部分個人情報の列
3412
3413
利用者暗号化部分個人情報を復号
3414
部分個人情報を出力

フロントページの続き

(51)Int.Cl.[7]	識別記号	ＦＩ	テーマコード(参考)
Ｇ０６Ｆ 17/60	５１２	Ｇ０６Ｆ 17/60	５１２

(72)発明者 高嶋 洋一
東京都千代田区大手町二丁目３番１号 日本電信電話株式会社内

Ｆターム(参考) 5B017 AA07 BA07 BA10 BB02 CA16
5B049 AA01 AA06 CC01 EE05
5B075 KK54 KK63 ND20 UU08